КОД безопасности

Средство защиты информации

Secret Net Studio – C

Руководство администратора

Установка, управление, мониторинг и аудит

RU.88338853.501400.002 91 1

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Список сокращений

AD	Active Directory
API	Application Programming Interface
ARP	Address Resolution Protocol
DDoS	Distributed Denial of Service
DNS	Domain Name System
GUID	Globally Unique Identifier
HTTPS	HyperText Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IIS	Intenet Information Services
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
LDS	Lightweight Directory Services
MBR	Master Boot Record
NTFS	New Technology File System
NTLM	NT LAN Manager
OSI	Open Systems Interconnection
PCI	Peripheral component interconnect
PCMCIA	Personal Computer Memory Card International Association
PIN	Personal Identification Number
RDP	Remote Desktop Protocol
RFC	Request for Comments
SCCM	System Center Configuration Manager
SIEM	Security Information and Event Management
SMBIOS	System management basic input/output system
SSL	Secure Socket Layer
SQL	Structured Query Language
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UEFI	Unified Extensible Firmware Interface
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
XML	eXtensible Markup Language
АК	Аппаратная конфигурация
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
АСУ ТП	Автоматизированная система управления производственными и технологическими процессами
БД	База данных

ГИС	Государственная информационная система
ЕБС	Единая биометрическая система
ЗПС	Замкнутая программная среда
ИС	Информационная среда
ИСПДн	Информационная система персональных данных
КИИ	Критическая информационная структура
КЦ	Контроль целостности
МЭ	Межсетевой экран
ОС	Операционная система
ОСР	Общедоступный сетевой ресурс
ОУ	Оперативное управление
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СБ	Сервер безопасности
СЗИ	Средство или система защиты информации
СПС	Справочно-правовая система
СУБД	Система управления базами данных
ФК	Функциональный контроль
ЦБД	Центральная база данных
ЦУ	Центр управления

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net Studio – C" RU.88338853.501400.002 (далее — Secret Net Studio, система защиты, изделие). В нем содержатся следующие сведения:

- принципы работы и возможности Secret Net Studio;
- порядок установки, обновления и удаления изделия;
- средства локального и централизованного управления системой защиты;
- средства мониторинга;
- порядок работы с централизованными журналами Secret Net Studio.

Условные обозначения

В руководстве для выделения некоторых элементов текста используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями.

Важная и дополнительная информация оформлена в виде примечаний.

Другие источники информации

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505-30-20 или по электронной почте support@securitycode.ru.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании https://www.securitycode.ru/company/education/training-courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте education@securitycode.ru.

Глава 1
Общие сведения о Secret Net Studio

Назначение системы

Система Secret Net Studio предназначена для обеспечения безопасности ИС на компьютерах, функционирующих под управлением ОС MS Windows 11/10/8/7 и Windows Server 2022/2019/2016/2012/2008.

При использовании соответствующих подсистем изделие обеспечивает:

- защиту от несанкционированного доступа к информационным ресурсам компьютеров;
- контроль устройств, подключаемых к компьютерам;
- межсетевое экранирование сетевого трафика;
- авторизацию сетевых соединений.

Управление функционированием системы Secret Net Studio может осуществляться централизованно или локально.

Основные функции

Система Secret Net Studio реализует следующие основные функции:

- Контроль входа пользователей в систему (идентификация и аутентификация пользователей).
- Дискреционное разграничение доступа к файловым ресурсам, устройствам, принтерам.
- Мандатное (полномочное) разграничение доступа к файловым ресурсам, устройствам, принтерам, сетевым интерфейсам, включая:
  - контроль потоков конфиденциальной информации в системе;
  - контроль вывода информации на съемные носители.
- Контроль состояния устройств компьютера с возможностями:
  - блокирования компьютера при изменении состояния заданных устройств;
  - блокирования подключения запрещенного устройства (устройства из запрещенной группы).
- Теневое копирование информации, выводимой на внешние носители и на печать.
- Автоматическая маркировка документов, выводимых на печать.
- Контроль целостности файловых объектов и реестра.
- Создание замкнутой программной среды для пользователей (контроль запуска исполняемых модулей, загрузки динамических библиотек, исполнения скриптов по технологии Active Scripts).
- Очистка оперативной и внешней памяти при ее перераспределении.
- Изоляция процессов (выполняемых программ) в оперативной памяти.
- Защита содержимого локальных жестких дисков при несанкционированной загрузке операционной системы.
- Шифрование данных на жестких дисках компьютера.
- Создание доверенной среды (внешний по отношению к ОС контроль работы ОС и системы защиты, установленных на компьютере).
- Межсетевое экранирование сетевого трафика.
- Авторизация сетевых соединений.

- Управление комплексом "Соболь" (управление пользователями, контролем целостности, получение событий безопасности).
- Функциональный контроль ключевых защитных подсистем.
- Самозащита от несанкционированных воздействий на ключевые защитные подсистемы.
- Регистрация событий безопасности.
- Централизованное и локальное управление параметрами работы механизмов защиты.
- Централизованное и локальное управление параметрами работы пользователей.
- Мониторинг и оперативное управление защищаемыми компьютерами.
- Централизованный сбор, хранение и архивирование журналов.

Состав устанавливаемых компонентов

Система Secret Net Studio состоит из следующих программных пакетов, устанавливаемых на компьютерах:

1. "Secret Net Studio" (далее — клиент).
2. "Secret Net Studio — Сервер безопасности" (далее — сервер безопасности или СБ).
3. "Secret Net Studio — Центр управления" (далее — Центр управления).

Клиент

Клиент системы Secret Net Studio предназначен для реализации защиты компьютера, на котором установлен данный компонент. Защита реализуется путем применения защитных механизмов, расширяющих и дополняющих средства безопасности ОС Windows. Защитные механизмы — это совокупность настраиваемых программных средств, входящих в состав клиента и обеспечивающих безопасное использование ресурсов.

Клиент может функционировать в следующих режимах:

- автономный режим — предусматривает только локальное управление защитными механизмами;
- сетевой режим — предусматривает локальное и централизованное управление защитными механизмами, а также централизованное получение информации и изменение состояния защищаемых компьютеров.

Режим функционирования определяется при установке клиентского ПО и может быть изменен в процессе эксплуатации клиента (см. стр.**213**).

Сервер безопасности

Сервер безопасности реализует возможности централизованного управления клиентами в сетевом режиме функционирования. Данный компонент обеспечивает:

- хранение данных централизованного управления;
- координацию работы других компонентов в процессе централизованного управления системой;
- получение и обработку информации о состоянии защищаемых компьютеров;
- управление пользователями и авторизацией сетевых соединений;
- централизованный сбор, хранение и архивирование журналов.

Центр управления

Центр управления используется для централизованного управления серверами безопасности и клиентами в сетевом режиме функционирования. Данный компонент обеспечивает:

- управление параметрами объектов;

- отображение информации о состоянии защищаемых компьютеров и произошедших событиях тревоги;
- загрузку журналов событий;
- оперативное управление компьютерами.

Лицензии на использование подсистем

Механизмы защиты системы Secret Net Studio доступны для использования при наличии соответствующих зарегистрированных лицензий. Лицензируются следующие механизмы:

- механизмы, входящие в базовую защиту (обязательная лицензия);
- дискреционное управление доступом;
- контроль устройств;
- затирание данных;
- замкнутая программная среда;
- полномочное управление доступом;
- контроль печати;
- защита дисков и шифрование данных;
- полнодисковое шифрование;
- межсетевой экран;
- авторизация сетевых соединений;
- паспорт ПО;
- доверенная среда;
- безопасная среда.

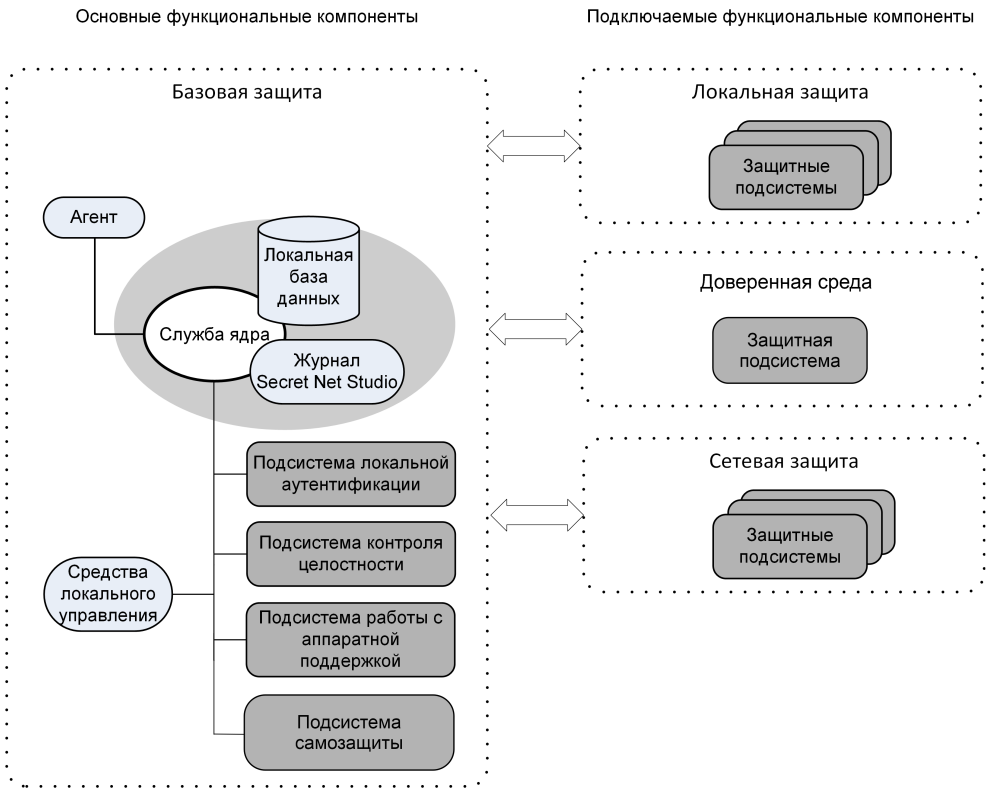
Глава 2
Составные части клиента

Группы функциональных компонентов клиента

В состав клиента системы Secret Net Studio входят следующие функциональные компоненты:

- основные программные службы, модули и защитные подсистемы (базовая защита);
- дополнительно подключаемые функциональные компоненты, условно разделенные на следующие группы:
  - локальная защита;
  - доверенная среда;
  - сетевая защита.

Обобщенная структурная схема клиента представлена на следующем рисунке.



Базовая защита

В базовую защиту входят следующие программные службы, модули и защитные подсистемы:

- ядро;
- агент;
- средства локального управления;
- подсистема локальной аутентификации;
- подсистема контроля целостности;
- подсистема работы с аппаратной поддержкой;
- подсистема самозащиты.

Ядро

Служба ядра автоматически запускается на защищаемом компьютере при его включении и функционирует на протяжении всего времени работы компьютера. Она осуществляет управление подсистемами и обеспечивает их взаимодействие.

Ядро выполняет следующие функции:

- обеспечивает обмен данными между подсистемами клиента и обработку поступающих команд;
- обеспечивает доступ других компонентов к информации, хранящейся в локальной базе данных Secret Net Studio;
- обрабатывает поступающую информацию о событиях, связанных с безопасностью системы, и регистрирует их в журнале Secret Net Studio.

Подсистема регистрации является одним из элементов ядра клиента. Она предназначена для управления регистрацией событий, связанных с работой системы защиты. Такие события регистрируются в журнале Secret Net Studio. Эта информация поступает от подсистем Secret Net Studio, которые следят за происходящими событиями. Перечень событий Secret Net Studio, подлежащих регистрации, устанавливается администратором безопасности.

В локальной БД Secret Net Studio хранится информация о настройках системы защиты, необходимых для работы защищаемого компьютера. Локальная БД размещается в реестре ОС Windows и специальных файлах.

Агент

Агентом является программный модуль в составе клиента, обеспечивающий взаимодействие с сервером безопасности. Агент принимает команды от сервера безопасности и отправляет ему данные о состоянии компьютера.

Агент используется только в сетевом режиме функционирования клиента.

Средства локального управления

Средства локального управления обеспечивают:

- управление объектами защиты (устройствами, файлами, каталогами);
- управление параметрами пользователей и защитных механизмов;
- формирование заданий на контроль целостности;
- просмотр локальных журналов.

Подсистема локальной аутентификации

Подсистема используется в механизме защиты входа в систему. Совместно с ОС Windows подсистема обеспечивает:

- проверку возможности входа пользователя в систему;
- оповещение пользователя о реализованных в системе мерах защиты информации и о последнем входе в систему;
- оповещение остальных модулей о начале или завершении работы пользователя;
- блокировку работы пользователя;
- загрузку данных с персональных идентификаторов пользователя;
- усиленную аутентификацию пользователя при входе в систему.

При обработке входа пользователя в систему осуществляется формирование контекста пользователя: определение его привилегий, уровня допуска и др. Дополнительно выполняется функциональный контроль работоспособности системы Secret Net Studio.

Подсистема контроля целостности

Подсистема контроля целостности обеспечивает проверку неизменности ресурсов компьютера: каталогов, файлов, ключей и значений реестра. В составе механизма контроля целостности подсистема реализует защиту от подмены ресурсов, сравнивая их с определенными эталонными значениями. Данная подсистема выполняет контролирующие функции не при обращении пользователя к ресурсам, а при наступлении определенных событий в системе (загрузка, вход пользователя, контроль по расписанию).

Подсистема работы с аппаратной поддержкой

Подсистема используется в механизме защиты входа в систему для работы с устройствами аппаратной поддержки. Она обеспечивает взаимодействие системы Secret Net Studio с определенным набором устройств и состоит из следующих модулей:

- модуль, обеспечивающий единый интерфейс обращения ко всем поддерживаемым устройствам аппаратной поддержки;
- модули работы с устройствами (каждый модуль обеспечивает работу с конкретным устройством);
- драйверы устройств аппаратной поддержки (если они необходимы).

Подсистема самозащиты

Данная подсистема обеспечивает функционирование механизма самозащиты (см. стр.**22**).

Подключаемые функциональные компоненты клиента

Локальная защита

К группе локальной защиты относятся подсистемы, реализующие применение следующих механизмов защиты:

- контроль устройств;
- контроль печати;
- замкнутая программная среда;
- полномочное управление доступом;
- дискреционное управление доступом к ресурсам файловой системы;
- затирание данных;
- защита информации на локальных дисках;
- шифрование данных на дисках;
- полнодисковое шифрование;
- шифрование данных в криптоконтейнерах;
- паспорт ПО.

Доверенная среда

Подсистема "Доверенная среда" реализует применение одноименного механизма защиты (см. стр.**38**).

Сетевая защита

К группе сетевой защиты относятся подсистемы, реализующие применение следующих механизмов защиты:

- межсетевой экран;
- авторизация сетевых соединений.

Глава 3
Механизмы защиты

Защита входа в систему

Защита входа в систему обеспечивает предотвращение доступа посторонних лиц к компьютеру. К механизму защиты входа относятся следующие средства:

- средства для идентификации и аутентификации пользователей;
- средства блокировки компьютера;
- аппаратные средства защиты от загрузки ОС со съемных носителей.

Идентификация и аутентификация пользователей

Идентификация и аутентификация пользователя выполняются при каждом входе в систему. Штатная для ОС Windows процедура входа предусматривает ввод имени и пароля пользователя или использование аппаратных средств, поддерживаемых операционной системой. Также возможен вход в систему с помощью учетной записи Microsoft и вход по графическому паролю.

В системе Secret Net Studio идентификация пользователей может выполняться в следующих режимах:

- "По имени" — для входа в систему пользователь может ввести свои учетные данные (имя и пароль) или использовать аппаратные средства, поддерживаемые ОС;
- "Смешанный" — для входа в систему пользователь может ввести свои учетные данные (имя и пароль) или использовать персональный идентификатор, поддерживаемый системой Secret Net Studio;
- "Только по идентификатору" — каждый пользователь для входа в систему должен обязательно использовать персональный идентификатор, поддерживаемый системой Secret Net Studio.

В качестве персональных идентификаторов в Secret Net Studio применяются средства идентификации и аутентификации на базе идентификаторов eToken, RuToken, JaCarta, ESMART или iButton. Чтобы использовать эти устройства, необходимо зарегистрировать их в системе защиты (присвоить пользователям).

Аутентификация пользователей может выполняться в усиленном режиме с дополнительной проверкой пароля пользователя системой Secret Net Studio. В режиме усиленной аутентификации пароли пользователей проверяются на соответствие требованиям политики паролей как в операционной системе, так и в Secret Net Studio.

Дополнительно для защиты компьютеров в Secret Net Studio предусмотрены следующие режимы:

- разрешение интерактивного входа только для доменных пользователей — в этом режиме блокируется вход в систему локальных пользователей (под локальными учетными записями);
- запрет вторичного входа в систему — в этом режиме блокируется запуск команд и сетевых подключений с вводом учетных данных другого пользователя (не выполнившего интерактивный вход в систему).

Блокировка компьютера

Средства блокировки компьютера предназначены для предотвращения несанкционированного использования компьютера. В этом режиме блокируется текущая сессия пользователя. Пока блокировка не снята, вход в систему разрешен только администратору.

Блокировка при неудачных попытках входа в систему

Для пользователей могут быть установлены ограничения на количество неудачных попыток входа в систему. В дополнение к стандартным возможностям ОС Windows (блокировка учетной записи пользователя после определенного числа попыток ввода неправильного пароля) система Secret Net Studio может контролировать неудачные попытки входа в систему при включенном режиме усиленной аутентификации по паролю. Если пользователь определенное количество раз вводит пароль, который не был сохранен в БД Secret Net Studio, — система блокирует компьютер. Разблокирование компьютера осуществляется администратором. Счетчик неудачных попыток обнуляется при удачном входе пользователя или после разблокирования компьютера.

Можно настроить временную блокировку при достижении максимального количества неудачных попыток входа в систему. В данном случае блокировка снимается по истечении заданного времени с момента последней неудачной попытки входа.

Временная блокировка компьютера

Режим временной блокировки включается в следующих случаях:

- если пользователь выполнил действие для включения блокировки;
- если истек заданный интервал неактивности (простоя) компьютера.

Для включения блокировки пользователь может применить стандартный способ блокировки рабочей станции или изъять свой идентификатор из считывателя. Чтобы выполнялась блокировка при изъятии идентификатора, администратору необходимо настроить реакцию на это действие в политиках с помощью программы управления. Блокировка при изъятии идентификатора выполняется при условии, что пользователь выполнил вход в систему с использованием этого идентификатора.

Блокировка по истечении заданного интервала неактивности осуществляется автоматически и распространяется на всех пользователей компьютера.

Для снятия временной блокировки необходимо указать пароль текущего пользователя или предъявить его идентификатор.

Блокировка компьютера при работе защитных подсистем

Блокировка компьютера предусмотрена и в алгоритмах работы защитных подсистем. Такой тип блокировки используется в следующих ситуациях:

- при нарушении функциональной целостности системы Secret Net Studio;
- при изменениях аппаратной конфигурации компьютера;
- при нарушении целостности контролируемых объектов.

Разблокирование компьютера в этих случаях осуществляется администратором.

Блокировка компьютера администратором оперативного управления

В сетевом режиме функционирования блокировка и разблокирование защищаемого компьютера могут осуществляться удаленно по команде пользователя Центра управления.

Аппаратные средства защиты

В Secret Net Studio поддерживается работа с аппаратными средствами, перечисленными в следующей таблице.

Аппаратные средства	Основные решаемые задачи
Средства идентификации и аутентификации на базе идентификаторов iButton, eToken, RuToken, JaCarta, ESMART, Guardant ID, vdToken	• Идентификация и аутентификация во время входа пользователя после загрузки ОС. • Идентификация и аутентификация во время входа пользователя с удаленного компьютера. • Снятие временной блокировки компьютера. • Хранение в идентификаторе пароля и криптографического ключа
ПАК "Соболь"	• Идентификация и аутентификация пользователей до загрузки ОС. • Идентификация и аутентификация во время входа пользователя после загрузки ОС. • Идентификация и аутентификация во время входа пользователя с удаленного компьютера. • Запрет загрузки ОС со съемных носителей. • Контроль целостности программной среды компьютера до загрузки ОС. • Снятие временной блокировки компьютера. • Хранение в идентификаторе пароля и криптографического ключа

Для идентификации и аутентификации пользователей могут применяться следующие средства:

- идентификаторы iButton (поддерживаемые типы DS1990 — DS1996). Считывающее устройство iButton подключается к разъему платы ПАК "Соболь";
- USB-ключи и смарт-карты (с любыми совместимыми USB-считывателями).

Полный список идентификаторов приведен в таблице ниже.

Продукт	USB-ключи	Смарт-карты
eToken PRO (Java)	eToken PRO (Java)	eToken PRO (Java) SC
JaCarta PKI	JaCarta PKI JaCarta PKI Flash	JaCarta PKI SC
JaCarta PKI/BIO	JaCarta PKI/BIO Jacarta-2 PKI/BIO/ГОСТ	JaCarta PKI/BIO JaCarta PKI/BIO/ГОСТ Jacarta-2 PKI/BIO/ГОСТ
JaCarta ГОСТ	JaCarta ГОСТ JaCarta PKI/ГОСТ JaCarta ГОСТ Flash	JaCarta ГОСТ SC
JaCarta-2 ГОСТ	JaCarta-2 ГОСТ JaCarta-2 PKI/ГОСТ	JaCarta-2 PKI/ГОСТ SC
JaCarta SF/ГОСТ	JaCarta SF/ГОСТ	—
JaCarta PRO	JaCarta PRO JaCarta-2 PRO/ГОСТ	JaCarta PRO SC JaCarta-2 PRO/ГОСТ SC
JaCarta WebPass	JaCarta WebPass	—
JaCarta-2 SE	JaCarta-2 SE	—
JaCarta U2F	JaCarta U2F	—
JaCarta LT	JaCarta LT	—
RuToken S	RuToken S (версия 2.0) RuToken S (версия 3.0)	—

Продукт	USB-ключи	Смарт-карты
RuToken ЭЦП	RuToken ЭЦП RuToken ЭЦП 2.0 RuToken ЭЦП Touch RuToken ЭЦП PKI RuToken ЭЦП 2.0 Flash RuToken ЭЦП Bluetooth RuToken ЭЦП 2.0 Touch RuToken ЭЦП 2.0 Flash Touch	RuToken ЭЦП SC RuToken ЭЦП 2.0 SC
RuToken Lite	RuToken Lite	RuToken Lite SC
RuToken 2151	RuToken 2151	RuToken 2151 SC
ESMART Token	ESMART Token	ESMART Token SC
ESMART Token ГОСТ	ESMART Token ГОСТ ESMART Token ГОСТ D	ESMART Token ГОСТ SC ESMART Token ГОСТ D SC
Guardant ID	Guardant ID Guardant ID 2.0	—
vdToken	vdToken 2.0	—
R301 Foros	R301 Foros	R301 Foros

Общие сведения об интеграции Secret Net Studio и комплексов "Соболь"

Secret Net Studio может функционировать совместно с ПАК "Соболь". При этом ПАК "Соболь" обеспечивает дополнительную защиту от несанкционированного доступа к информационным ресурсам компьютера, на котором установлена система Secret Net Studio.

Примечание. В Secret Net Studio версии 8.4 и ниже реализована интеграция с ПАК "Соболь" версий 3.x.

В Secret Net Studio версии 8.5 и выше реализована интеграция с ПАК "Соболь" версии 4. ПАК "Соболь" версии 4 является новым поколением продуктовой линейки ПАК "Соболь", архитектура и интерфейс которого значительно отличаются от ПАК "Соболь" версий 3.x. Особенности совместной работы Secret Net Studio с ПАК "Соболь" версии 4 будут указаны отдельно либо в примечании к имеющимся в руководствах сведениям.

В ПАК "Соболь" для интеграции с Secret Net Studio реализован режим совместного использования. Также ПАК "Соболь" может функционировать самостоятельно в автономном режиме.

В автономном режиме работы ПАК "Соболь" реализует свои основные функции до старта операционной системы независимо от Secret Net Studio. Управление пользователями, журналом регистрации событий, настройка общих параметров осуществляются средствами администрирования комплекса без ограничений.

В режиме совместного использования (интеграции) значительная часть функций управления комплексом осуществляется средствами администрирования Secret Net Studio. Перечень функций представлен в следующей таблице.

Функция	Описание
Управление входом пользователя Secret Net Studio в ПАК "Соболь" с помощью идентификатора, инициализированного и присвоенного пользователю в системе Secret Net Studio	Пользователю предоставляются права на автоматический вход в комплекс и далее в систему при однократном предъявлении идентификатора. Также для входа может использоваться пароль, записанный в память персонального идентификатора
Управление работой подсистемы контроля целостности ПАК "Соболь"	Для ПАК "Соболь" задания на контроль целостности файлов жесткого диска и объектов реестра формируются средствами администрирования Secret Net Studio

Функция	Описание
Управление параметрами ПАК "Соболь"	Значения параметров "Минимальная длина пароля" и "Количество неудачных попыток аутентификации", установленные в Secret Net Studio, передаются в ПАК "Соболь"
Автоматическая передача записей журнала регистрации событий ПАК "Соболь" в журнал Secret Net Studio	Передача записей и их преобразование осуществляются автоматически при загрузке подсистемы аппаратной поддержки Secret Net Studio

Подробные сведения о реализации этих функций содержатся в документе [**2**], раздел "Использование ПАК "Соболь" в режиме интеграции с Secret Net Studio".

Внимание!

- В режиме интеграции системы Secret Net Studio и комплекса "Соболь" идентификатор iButton DS1992 не используется. Рекомендуется использовать идентификаторы DS1995, DS1996 или USB-ключи и смарт-карты, поддерживаемые ПАК "Соболь".
- Для использования Secret Net Studio совместно с комплексом "Соболь" необходимо установить вспомогательное ПО комплекса (см. документацию на изделие).

Для обеспечения защиты данных в процессе централизованного управления ПАК "Соболь" в Secret Net Studio реализован ряд криптографических преобразований на основе ГОСТ 28147– 89, ГОСТ Р 34.10– 2001. Перечень используемых ключей шифрования представлен в следующей таблице.

Наименование ключа	Назначение	Место хранения
Симметричный ключ ЦУ	Шифрование аутентификаторов[1] в хранилище объектов централизованного управления Secret Net Studio. Расчет имитовставки для списка доступных пользователю компьютеров	Персональный идентификатор администратора
Закрытый ключ ЦУ	Расчет сессионного ключа компьютера при выполнении операций администрирования	-"-
Открытый ключ ЦУ	Расчет сессионного ключа компьютера при выполнении операций синхронизации	Локальная база данных управляемого компьютера
Закрытый ключ компьютера	Расчет сессионного ключа компьютера при выполнении операций синхронизации	-"-
Открытый ключ компьютера	Расчет сессионного ключа компьютера при выполнении операций администрирования	Служба каталогов
Сессионный ключ компьютера	Шифрование информации, предназначенной для защищаемого компьютера	Не хранится (вычисляется в процессе работы)
Ключ преобразования паролей комплексов "Соболь"	В ПАК "Соболь" версий 3.x — шифрование информации в закрытой памяти платы комплекса "Соболь". В ПАК "Соболь" версий 3.x и 4 — шифрование информации, хранящейся в локальной базе данных защищаемого компьютера	В ПАК "Соболь" версий 3.x — закрытая память платы комплекса "Соболь". В ПАК "Соболь" версии 4 — локальная база данных управляемого компьютера
Уникальный номер платы[2]	Расшифрование информации из открытой памяти платы комплекса "Соболь". Подпись внешних запросов	Локальная база данных управляемого компьютера

[1] Аутентификатор — структура данных, хранящаяся в службе каталогов, которая совместно с паролем пользователя используется в процедуре его аутентификации.

[2] Только для интеграции с ПАК "Соболь" версии 4.

Функциональный контроль подсистем

Функциональный контроль предназначен для обеспечения гарантии того, что к моменту входа пользователя в ОС (т. е. к моменту начала работы пользователя) все ключевые защитные подсистемы загружены и функционируют.

В случае успешного завершения функционального контроля этот факт регистрируется в журнале Secret Net Studio.

При неуспешном завершении функционального контроля в журнале Secret Net Studio регистрируется событие с указанием причин (это возможно при условии работоспособности ядра Secret Net Studio). Вход в систему разрешается только пользователям, входящим в локальную группу администраторов компьютера.

Одной из важных задач функционального контроля является обеспечение защиты ресурсов компьютера при запуске ОС в безопасном режиме (Safe mode). Безопасный режим запуска не является штатным режимом функционирования для системы Secret Net Studio, однако при необходимости администратор может его использовать для устранения неполадок. Поскольку в безопасном режиме не действуют некоторые функции системы защиты, функциональный контроль в этих условиях завершается с ошибкой. В результате блокируется вход любых пользователей, кроме администраторов. Поэтому при надлежащем соблюдении правил политики безопасности, когда никто из обычных пользователей не обладает полномочиями администратора, доступ к ресурсам компьютера в обход механизмов защиты невозможен.

Самозащита

Механизм самозащиты предотвращает несанкционированную остановку критических служб и процессов и выгрузку драйверов Secret Net Studio, обеспечивает защиту программных модулей и ключей системного реестра, необходимых для работы Secret Net Studio, от несанкционированной модификации или удаления. Также дополнительно может осуществляться контроль доступа пользователей с правами локального администратора компьютера к следующим средствам управления:

- Локальный центр управления;
- программа "Контроль программ и данных (централизованный режим)";
- программа "Контроль программ и данных" в локальном режиме;
- программа дополнительной настройки подсистемы полномочного управления доступом;
- Центр управления пользователями;
- программа установки клиента в режиме удаления;
- диалоговое окно "Управление Secret Net Studio" в Панели управления Windows.

События, связанные с функционированием механизма самозащиты, регистрируются в журнале Secret Net Studio.

Управление механизмом самозащиты может выполняться централизованно в Центре управления или непосредственно на защищаемом компьютере в Локальном центре управления. Управлять механизмом могут только пользователи, обладающие необходимыми привилегиями.

Для экстренных случаев предусмотрена возможность переключения механизма самозащиты в сервисный режим. Переключение выполняется с помощью утилиты командной строки в защищенном или обычном режиме работы ОС Windows.

Регистрация событий

В процессе работы системы Secret Net Studio события, происходящие на компьютере и связанные с безопасностью системы, регистрируются в журнале Secret Net Studio. Все записи журнала хранятся в файле на системном диске. Формат данных идентичен формату журнала безопасности ОС Windows.

Имеется возможность настройки перечня регистрируемых событий и параметров хранения журнала. Это позволяет обеспечить оптимальный объем сохраняемых сведений с учетом размера журнала и нагрузки на систему.

Контроль целостности

Механизм контроля целостности осуществляет слежение за неизменностью контролируемых объектов. Контроль проводится в автоматическом режиме в соответствии с заданным расписанием.

Объектами контроля могут быть файлы, каталоги, элементы системного реестра (настраиваются с помощью средств Secret Net Studio), а также секторы дисков, PCI-устройства и структуры SMBIOS (только при использовании ПАК "Соболь"). Каждый тип объектов имеет свой набор контролируемых параметров.

В системе предусмотрена возможность настройки периодичности контроля по определенным дням и времени в течение дня. Запуск процесса контроля может выполняться при загрузке ОС, при входе пользователя в систему или после входа.

При проверке целостности могут применяться различные варианты реакции системы на выполнение заданий контроля. Можно настраивать регистрацию определенных типов событий (успех или ошибка проверки отдельного объекта либо всего задания контроля) и действия в случае нарушения целостности (игнорировать ошибку, заблокировать компьютер, принять новое значение как эталон).

Вся информация об объектах, методах, расписаниях контроля сосредоточена в специальной структуре, которая называется модель данных. Модель данных хранится в локальной базе данных системы Secret Net Studio и представляет собой иерархический список объектов с описанием связей между ними. Используются следующие категории объектов в порядке от низшего уровня иерархии к высшему:

- ресурсы;
- группы ресурсов;
- задачи;
- задания;
- субъекты управления (компьютеры, пользователи, группы компьютеров и пользователей).

Модель данных является общей для механизмов контроля целостности и замкнутой программной среды.

Управление локальными моделями данных на защищаемых компьютерах можно осуществлять централизованно (для клиентов в сетевом режиме функционирования). Для централизованного управления в глобальном каталоге создаются две модели данных — для компьютеров под управлением 32-разрядных версий ОС Windows и для компьютеров с 64- разрядными версиями операционных систем. Такое разделение позволяет учитывать специфику используемого ПО на защищаемых компьютерах с различными платформами.

Каждая из централизованных моделей данных является общей для всех защищаемых компьютеров под управлением версий ОС Windows соответствующей разрядности (32- или 64-разрядные версии). При изменении параметров централизованной модели выполняется локальная синхронизация этих изменений на защищаемом компьютере. Новые параметры из централизованного хранилища передаются на компьютер, помещаются в локальную модель данных и затем используются защитными механизмами.

Синхронизация может выполняться в следующие моменты:

- при загрузке компьютера;
- при входе пользователя в систему;
- после входа (в фоновом режиме во время работы пользователя);
- периодически через определенные интервалы времени;
- принудительно по команде администратора;
- непосредственно после внесения изменений в ЦБД КЦ-ЗПС.

Редактирование централизованных моделей данных осуществляется со следующими особенностями: для изменения доступна та модель данных, которая соответствует разрядности ОС Windows на рабочем месте администратора. Модель данных другой разрядности доступна только для чтения (при этом можно экспортировать данные из этой модели в другую). Таким образом, если в системе имеются защищаемые компьютеры с версиями ОС различной разрядности, для централизованного управления моделями данных администратору следует организовать два рабочих места — на компьютере с 32-разрядной версией и на компьютере с 64-разрядной версией ОС Windows.

Дискреционное управление доступом к ресурсам файловой системы

В состав системы Secret Net Studio входит механизм дискреционного управления доступом к ресурсам файловой системы. Этот механизм обеспечивает:

- разграничение доступа пользователей к каталогам и файлам на локальных дисках на основе матрицы доступа субъектов (пользователей, групп) к объектам доступа;
- контроль доступа к объектам при локальных или сетевых обращениях, включая обращения от имени системной учетной записи;
- невозможность доступа к объектам в обход установленных прав доступа (если используются стандартные средства ОС или прикладные программы без собственных драйверов для работы с файловой системой);
- независимость действия от встроенного механизма избирательного разграничения доступа ОС Windows. То есть установленные права доступа к файловым объектам в системе Secret Net Studio не влияют на аналогичные права доступа в ОС Windows и наоборот.

Аналогично реализации в ОС Windows матрица доступа в системе Secret Net Studio представляет собой списки файловых объектов, в которых определены учетные записи с правами доступа. Права устанавливают разрешения или запреты на выполнение операций. Перечень предусмотренных прав доступа представлен в следующей таблице.

Право доступа	Действие для каталога	Действие для файла
Чтение (R)	Разрешает или запрещает просмотр имен файлов и подкаталогов	Разрешает или запрещает чтение данных
	Разрешает или запрещает просмотр атрибутов файлового объекта	

Право доступа	Действие для каталога	Действие для файла
Запись (W)	Разрешает или запрещает создание подкаталогов и файлов	Разрешает или запрещает внесение изменений
	Разрешает или запрещает смену атрибутов файлового объекта	
Выполнение (X)	Разрешает или запрещает перемещение по структуре подкаталогов	Разрешает или запрещает выполнение
Удаление (D)	Разрешает или запрещает удаление файлового объекта	
Изменение прав доступа (P)	Разрешает или запрещает изменение прав доступа к файловому объекту. Пользователь, имеющий разрешение на изменение прав доступа к ресурсу, условно считается администратором ресурса	

Права доступа для файлового объекта могут быть заданы явно или наследоваться от вышестоящего элемента иерархии. Явно заданные права имеют более высокий приоритет по сравнению с наследуемыми правами. Права доступа считаются заданными явно, если для объекта отключен режим наследования прав.

Для управления списками доступа к любым файловым объектам предусмотрена специальная привилегия "Дискреционное управление доступом: Учетные записи с привилегией управления правами доступа". Пользователи, обладающие этой привилегией, могут изменять права доступа для всех каталогов и файлов на локальных дисках (независимо от установленных прав доступа к объектам).

По умолчанию привилегией на управление правами доступа обладают пользователи, входящие в локальную группу администраторов. При этом для всех пользователей действуют разрешающие права доступа к любым ресурсам на чтение, запись, выполнение и удаление (RWXD). Эти права наследуются от корневых каталогов логических разделов. Во избежание непреднамеренной блокировки работы ОС, которая может произойти из-за некорректно установленных прав доступа к ресурсам, — отсутствует возможность изменения прав доступа для корневого каталога системного диска (%SystemDrive%) и всего системного каталога (%SystemRoot%).

Копирование и перемещение файловых объектов

При копировании файлового объекта для его копии принудительно включается режим наследования прав доступа, даже если оригинальный объект обладает явно заданными правами.

Перемещение файлового объекта в пределах своего логического раздела осуществляется с сохранением явно заданных прав доступа для этого объекта. Если для объекта включен режим наследования — после перемещения вступают в действие права того каталога, в который перемещен объект. При перемещении объекта в другой логический раздел принудительно включается режим наследования прав.

Аудит операций с файловыми объектами

При работе механизма дискреционного управления доступом в журнале Secret Net Studio могут регистрироваться события успешного доступа к объектам, запрета доступа или изменения прав. По умолчанию регистрация событий успешного доступа не осуществляется, а события запрета доступа и изменения прав регистрируются для всех файловых объектов. Включение и отключение регистрации указанных событий осуществляется администратором безопасности при настройке параметров групповых политик.

Для файловых объектов можно детализировать аудит по выполняемым операциям, которые требуют определенных прав доступа. Например, включить аудит успешного доступа при выполнении операций записи в файл или его удаления. Включение и отключение аудита операций может выполнять администратор ресурса при настройке дополнительных параметров прав доступа к файловому объекту.

Затирание удаляемой информации

Затирание удаляемой информации делает невозможным восстановление и повторное использование данных после их удаления. Гарантированное уничтожение достигается путем записи случайных последовательностей чисел на место удаленной информации в освобождаемой области памяти.

В Secret Net Studio – C реализованы следующие варианты затирания информации:

- автоматическое затирание при удалении данных с устройств определенных типов (локальные и сменные диски, оперативная память) при включении функции затирания в Центре управления;

  Примечание. В Secret Net Studio – C реализована возможность исключения выбранных объектов (файлов и папок) из обработки при автоматическом затирании данных на локальных дисках и сменных носителях посредством создания списка исключений.

- затирание при удалении файловых объектов, выбранных пользователем, по команде из контекстного меню;
- затирание по команде из контекстного меню пиктограммы Secret Net Studio в панели задач Windows всех данных (включая таблицу разделов, логические тома, файловые объекты и остаточную информацию) на локальных дисках (кроме системного диска) и сменных носителях, подключенных к защищаемому компьютеру.

Для большей надежности может быть выполнено несколько циклов (проходов) затирания.

При настройке механизма можно установить различное количество циклов затирания для:

- локальных и сменных дисков, оперативной памяти;
- файловых объектов, удаляемых с помощью специальной команды;
- носителей информации при уничтожении всех данных на них.

Внимание! Затирание файла подкачки виртуальной памяти выполняется стандартными средствами ОС Windows при выключении компьютера. Если в Secret Net Studio включен режим затирания оперативной памяти, рекомендуется дополнительно в политиках Windows включить действие стандартного параметра "Завершение работы: очистка файла подкачки виртуальной памяти" (размещается в разделе Конфигурация компьютера\Параметры Windows\Параметры безопасности \Локальные политики\Параметры безопасности).

Не осуществляется затирание файлов при их перемещении в папку "Корзина", так как во время нахождения в этой папке файлы не удаляются с диска. Затирание таких файлов происходит после очистки содержимого папки "Корзина".

Для снижения нагрузки на компьютер при удалении большого объема данных с локальных дисков и сменных носителей в Secret Net Studio реализован механизм отложенного затирания. Остаточные данные, подлежащие затиранию, добавляются в очередь на обработку. Затирание выполняется в порядке очереди, с временной задержкой, и завершается до выключения компьютера.

Контроль подключения и изменения устройств компьютера

Механизм контроля подключения и изменения устройств компьютера обеспечивает:

- своевременное обнаружение изменений аппаратной конфигурации компьютера и реагирование на эти изменения;
- поддержание в актуальном состоянии списка устройств компьютера, который используется механизмом разграничения доступа к устройствам.

Изменения аппаратной конфигурации отслеживаются системой защиты для устройств с включенным режимом контроля "Устройство постоянно подключено к компьютеру".

Начальная аппаратная конфигурация компьютера определяется на этапе установки системы. При этом значения параметров контроля задаются по умолчанию. Настройку политики контроля можно выполнить индивидуально для каждого устройства или применять к устройствам наследуемые параметры от моделей, классов и групп, к которым относятся устройства.

Используются следующие методы контроля конфигурации:

- Статический контроль конфигурации. Каждый раз при загрузке компьютера подсистема получает информацию об актуальной аппаратной конфигурации и сравнивает ее с эталонной.
- Динамический контроль конфигурации. Во время работы компьютера (а также при выходе из спящего режима) драйвер-фильтр устройств отслеживает факты подключения, отключения или изменения параметров устройств. Если произошло изменение конфигурации, драйвер-фильтр выдает оповещение об этом и система выполняет определенные действия (например, блокировку компьютера).

При обнаружении изменений аппаратной конфигурации система ожидает утверждения этих изменений администратором безопасности. Процедура утверждения аппаратной конфигурации необходима для санкционирования обнаруженных изменений и принятия текущей аппаратной конфигурации в качестве эталонной.

Разграничение доступа к устройствам

Разграничение доступа пользователей к устройствам выполняется на основании списков устройств, которые формируются механизмом контроля подключения и изменения устройств (см. стр.**27**).

Система Secret Net Studio предоставляет следующие возможности для разграничения доступа пользователей к устройствам:

- установка стандартных разрешений и запретов на выполнение операций с устройствами;
- назначение устройствам категорий конфиденциальности или допустимых уровней конфиденциальности сессий пользователей — чтобы разграничить доступ с помощью механизма полномочного управления доступом.

Возможности по разграничению доступа зависят от типов устройств. Разграничение не осуществляется полностью или частично для устройств, имеющих особую специфику использования или необходимых для работы компьютера. Например, не ограничивается доступ к процессору и оперативной памяти, ограничены возможности разграничения доступа для портов ввода/вывода.

Для устройств с отключенным режимом контроля или запрещенных для подключения не действует разграничение доступа по установленным разрешениям и запретам на выполнение операций. Права доступа пользователей к таким устройствам не контролируются.

При установке клиентского ПО системы Secret Net Studio выставляются права доступа для всех обнаруженных устройств, поддерживающих такое разграничение доступа. По умолчанию предоставляется полный доступ трем стандартным группам пользователей: "Система", "Администраторы" и "Все". То есть всем пользователям разрешен доступ без ограничений ко всем устройствам, обнаруженным на компьютере. Далее администратор безопасности разграничивает доступ пользователей к устройствам в соответствии с требованиями политики безопасности. Для этого можно выполнить настройку прав доступа непосредственно для устройств или для классов и групп, к которым они относятся.

Настройка прав доступа для классов и групп позволяет подготовить систему защиты к возможным подключениям новых устройств. При подключении новое устройство включается в соответствующую группу, класс и модель (если есть). Доступ пользователей к этому устройству будет разграничен автоматически — в соответствии с правилами, которые установлены для группы, класса или модели.

Разграничение доступа пользователей к устройствам с назначенными категориями конфиденциальности или уровнями конфиденциальности сессий осуществляется механизмом полномочного управления доступом.

Замкнутая программная среда

Механизм замкнутой программной среды позволяет определить для любого пользователя компьютера индивидуальный перечень программного обеспечения, разрешенного для использования. Система защиты контролирует и обеспечивает запрет использования следующих ресурсов:

- файлы запуска программ и библиотек, не входящие в перечень разрешенных для запуска и не удовлетворяющие определенным условиям;
- сценарии, не входящие в перечень разрешенных для запуска и не зарегистрированные в базе данных.

Примечание. Сценарий (называемый также скрипт) представляет собой последовательность исполняемых команд и/или действий в текстовом виде. Система Secret Net Studio контролирует выполнение сценариев, созданных по технологии Active Scripts.

Попытки запуска неразрешенных ресурсов регистрируются в журнале как события тревоги.

На этапе настройки механизма составляется список ресурсов, разрешенных для запуска и выполнения. Список может быть сформирован автоматически на основании сведений об установленных на компьютере программах или по записям журналов (журнал безопасности или журнал Secret Net Studio), содержащих сведения о запусках программ, библиотек и сценариев.

Для файлов, входящих в список, можно включить проверку целостности с использованием механизма контроля целостности (см. стр.**23**). По этой причине механизм замкнутой программной среды и механизм контроля целостности используют единую модель данных.

Механизм замкнутой программной среды не осуществляет блокировку запускаемых программ, библиотек и сценариев в следующих случаях:

- при наличии у пользователя привилегии "Замкнутая программная среда: Не действует" — контроль запускаемых пользователем ресурсов не осуществляется;
- при включенном мягком режиме работы подсистемы замкнутой программной среды — в этом режиме контролируются попытки запуска программ, библиотек и сценариев, но разрешается использование любого ПО. Данный режим обычно используется на этапе настройки механизма.

Изоляция процессов

В системе Secret Net Studio может применяться режим изоляции процессов для предотвращения стороннего доступа к данным определенных исполняемых модулей. При действующем режиме контролируются следующие операции с данными, которыми обмениваются различные процессы:

- чтение данных из буфера обмена;
- чтение данных в окне другого процесса;
- запись данных в окно другого процесса;
- перемещение данных между процессами методом drag-and-drop.

Процесс считается изолированным, если в модели данных включена изоляция для ресурса, являющегося исполняемым файлом этого процесса. Для изолированного процесса обмен данными с другими процессами невозможен. Разрешается использование буфера обмена только при записи и чтении данных одного и того же процесса. Неизолированные процессы обмениваются данными без ограничений.

Изоляция процессов реализуется при включенном механизме замкнутой программной среды (должен функционировать драйвер механизма). Режим работы механизма ЗПС может быть любым. При этом для исключения возможностей запуска копий исполняемых файлов в неизолированной среде рекомендуется настроить механизм ЗПС и включить жесткий режим работы механизма.

Полномочное управление доступом

Механизм полномочного управления доступом обеспечивает:

- разграничение доступа пользователей к информации, которой назначена категория конфиденциальности (конфиденциальная информация);
- контроль подключения и использования устройств с назначенными категориями конфиденциальности;
- контроль потоков конфиденциальной информации в системе;
- контроль отображения конфиденциальных файлов в менеджерах файлов;
- контроль использования сетевых интерфейсов, для которых указаны допустимые уровни конфиденциальности сессий пользователей;
- контроль печати конфиденциальных документов.

По умолчанию в системе предусмотрены категории конфиденциальности: "неконфиденциально", "конфиденциально" и "строго конфиденциально". При необходимости можно увеличить количество используемых категорий и задать для них названия в соответствии со стандартами, принятыми в вашей организации. Максимально возможное количество категорий — 16.

Категорию конфиденциальности можно назначить для следующих ресурсов:

- локальные физические диски (кроме диска с системным логическим разделом) и любые устройства, включаемые в группы устройств USB, PCMCIA, IEEE1394 или Secure Digital;
- каталоги и файлы на локальных физических дисках.

Пояснение. Каталогам и файлам, находящимся на устройствах из групп USB, PCMCIA, IEEE1394, Secure Digital (сменные носители), категория конфиденциальности непосредственно не назначается. Для них действует категория конфиденциальности, назначенная устройству.

Доступ пользователя к конфиденциальной информации осуществляется в соответствии с его уровнем допуска. Если уровень допуска пользователя ниже, чем категория конфиденциальности ресурса, то система блокирует доступ к этому ресурсу. После получения доступа к конфиденциальной информации уровень конфиденциальности программы (процесса) повышается до категории конфиденциальности ресурса. Это необходимо для того, чтобы исключить возможность сохранения конфиденциальных данных в файлах с меньшей категорией конфиденциальности.

Предусмотрен режим работы механизма полномочного управления доступом, при котором пользователь в различных менеджерах файлов увидит только те файлы, категория конфиденциальности которых не превышает его права доступа к конфиденциальным ресурсам. Файлы с более высокими категориями конфиденциальности пользователю показаны не будут. В режиме контроля потоков права пользователя определяются уровнем конфиденциальности сессии.

Полномочное разграничение доступа на уровне устройств осуществляется следующим образом. Если устройство подключается во время сеанса работы пользователя с уровнем допуска ниже, чем категория устройства, система блокирует подключение устройства. При подключении такого устройства до начала сеанса работы пользователя — запрещается вход пользователя в систему. В режиме контроля потоков уровень конфиденциальности сессии пользователя должен соответствовать категориям всех подключенных устройств.

Функционирование устройства разрешено независимо от уровня допуска пользователя, если для этого устройства включен режим "без учета категории конфиденциальности". Данный режим включен по умолчанию.

Доступ к содержимому конфиденциального файла предоставляется пользователю, если категория файла не превышает уровень допуска пользователя. При этом также учитывается категория конфиденциальности устройства.

Категория конфиденциальности локального физического диска имеет более высокий приоритет, чем категории файлов (каталогов), расположенных на этом устройстве. Если категория файла (каталога) ниже категории конфиденциальности устройства, система считает категорию файла (каталога) равной категории устройства. Если же категория файла (каталога) превышает категорию конфиденциальности устройства, такое состояние считается некорректным и доступ к файлу (каталогу) запрещается.

Режим контроля потоков

При использовании механизма в режиме контроля потоков конфиденциальной информации всем процессам обработки данных в системе присваивается единый уровень конфиденциальности. Нужный уровень конфиденциальности из числа доступных пользователю выбирается перед началом сессии работы на компьютере. Этот уровень нельзя изменить до окончания сессии.

В режиме контроля потоков сохранение информации разрешено только с категорией, равной уровню конфиденциальности сессии. Полностью запрещается доступ к данным, категория которых превышает уровень конфиденциальности сессии (даже если уровень допуска пользователя позволяет доступ к таким данным). Таким образом, режим контроля потоков обеспечивает строгое соблюдение принципов полномочного разграничения доступа и предотвращает несанкционированное копирование или перемещение конфиденциальной информации.

В режиме контроля потоков запрещается использование устройств, которым назначена категория конфиденциальности, отличающаяся от выбранного уровня сессии. Если на момент входа пользователя к компьютеру подключены устройства с различными категориями конфиденциальности, вход запрещается по причине конфликта подключенных устройств. Использование устройств, которым назначена категория конфиденциальности выше, чем уровень допуска пользователя, ограничивается так же, как и при отключенном режиме контроля потоков.

Режим контроля потоков позволяет установить ограничения на использование сетевых интерфейсов. Для каждого сетевого интерфейса можно выбрать уровни конфиденциальности сессий, в которых этот интерфейс будет доступен пользователю. Если открыта сессия с другим уровнем конфиденциальности, функционирование этого интерфейса блокируется системой защиты. Это позволяет организовать работу пользователя в различных сетях в зависимости от выбранного уровня конфиденциальности сессии.

Для сетевых интерфейсов предусмотрен режим доступности "Адаптер доступен всегда" (включен по умолчанию). В этом режиме функционирование сетевого интерфейса разрешено независимо от уровня конфиденциальности сессии.

Скрытие конфиденциальных файлов

Если включен режим скрытия недоступных конфиденциальных файлов, пользователь не будет видеть в менеджерах файлов те файлы, категория конфиденциальности которых превышает текущий уровень конфиденциальности сессии.

Вывод конфиденциальной информации

Механизм полномочного управления доступом осуществляет контроль вывода конфиденциальной информации на внешние носители. Внешними носителями в системе Secret Net Studio считаются сменные диски, для которых включен режим доступа "без учета категории конфиденциальности". При копировании или перемещении конфиденциального ресурса на такой носитель не сохраняется его категория конфиденциальности. Поэтому чтобы осуществлять вывод конфиденциальной информации на внешние носители в режиме контроля потоков, пользователь должен обладать соответствующей привилегией.

Для предотвращения несанкционированного вывода конфиденциальных документов на локальные и сетевые принтеры используется механизм контроля печати. Механизм обеспечивает вывод конфиденциальных документов на печать только при наличии соответствующей привилегии. Также в распечатываемые документы может автоматически добавляться специальный маркер (гриф), в котором указывается категория конфиденциальности документа. События печати регистрируются в журнале Secret Net Studio.

Контроль печати

Механизм контроля печати обеспечивает:

- разграничение доступа пользователей к принтерам;
- регистрацию событий вывода документов на печать в журнале Secret Net Studio;
- вывод на печать документов с определенной категорией конфиденциальности;
- автоматическое добавление грифа в распечатываемые документы (маркировка документов);
- теневое копирование распечатываемых документов.

Для реализации функций маркировки и/или теневого копирования распечатываемых документов в систему добавляются драйверы "виртуальных принтеров". Виртуальные принтеры соответствуют реальным принтерам, установленным на компьютере. Список виртуальных принтеров автоматически формируется при включении контроля печати и режима теневого копирования. Печать в этом случае разрешается только на виртуальные принтеры.

При печати на виртуальный принтер выполняются дополнительные преобразования для получения образа распечатываемого документа в формате XML Paper Specification (XPS). Далее XPS-документ копируется в хранилище теневого копирования (если для принтера включена функция теневого копирования), модифицируется нужным образом и после этого передается для печати в соответствующее печатающее устройство.

Теневое копирование выводимых данных

Механизм теневого копирования обеспечивает создание в системе дубликатов данных, выводимых на съемные носители информации. Дубликаты (копии) сохраняются в специальном хранилище, доступ к которому имеют только уполномоченные пользователи. Действие механизма распространяется на те устройства, для которых включен режим сохранения копий при записи информации.

При включенном режиме сохранения копий вывод данных на внешнее устройство возможен только при условии создания копии этих данных в хранилище теневого копирования. Если по каким-либо причинам создать дубликат невозможно, операция вывода данных блокируется.

Теневое копирование поддерживается для устройств следующих видов:

- подключаемые сменные диски;
- дисководы гибких дисков;
- дисководы оптических дисков с функцией записи;
- принтеры.

При выводе данных на подключаемый сменный диск в хранилище теневого копирования создаются копии файлов, записанных на носитель в ходе операции вывода. Если файл открыт для редактирования непосредственно со сменного носителя, при сохранении новой версии файла в хранилище будет создан его отдельный дубликат.

Для устройства записи оптических дисков механизм теневого копирования создает в хранилище образ диска, если для записи используется интерфейс Image Mastering API (IMAPI), или копии файлов, если запись осуществляется в формате файловой системы Universal Disk Format (UDF).

Внимание! Некоторые программные пакеты, имеющие функцию записи оптических дисков, используют собственные драйверы управления устройствами. Такие драйверы могут осуществлять доступ к устройству в обход механизма теневого копирования. Для обеспечения гарантированного контроля запись дисков необходимо осуществлять только с использованием штатных средств ОС Windows.

Теневое копирование распечатываемых документов осуществляется с использованием механизма контроля печати (см. стр. **31**). В качестве копии выводимой на печать информации сохраняется образ печатаемого документа в формате XPS (сокр. от XML Paper Specification) — открытый графический формат фиксированной разметки на базе языка XML, разработанный компанией Microsoft.

Контроль вывода данных с помощью механизма теневого копирования является одной из задач аудита. События вывода данных регистрируются в журнале Secret Net Studio. Доступ к дубликатам в хранилище теневого копирования осуществляется с помощью Локального центра управления. Программа предоставляет средства для поиска по содержимому хранилища.

Администратор настраивает функционирование механизма теневого копирования в Центре управления. При настройке определяются параметры хранилища теневого копирования, а также включается или отключается действие механизма для устройств или принтеров.

Защита информации на локальных дисках

Механизм защиты информации на локальных дисках компьютера (механизм защиты дисков) предназначен для блокирования доступа к жестким дискам при несанкционированной загрузке компьютера. Загрузка считается санкционированной, если она выполнена средствами операционной системы с установленным клиентским ПО Secret Net Studio. Все другие способы загрузки ОС считаются несанкционированными (например, загрузка с внешнего носителя или загрузка другой ОС, установленной на компьютере).

Механизм обеспечивает защиту информации при попытках доступа, осуществляемых с помощью штатных средств операционной системы.

Действие механизма защиты дисков основано на модификации загрузочных секторов (boot-секторов) логических разделов на жестких дисках компьютера. Содержимое загрузочных секторов модифицируется путем кодирования с использованием специального ключа, который автоматически генерируется при включении механизма. При этом часть служебных данных для механизма защиты дисков сохраняется в системном реестре.

Модификация позволяет скрыть информацию о логических разделах при несанкционированной загрузке компьютера — разделы с модифицированными загрузочными секторами будут восприниматься системой как неформатированные или поврежденные. При санкционированной загрузке компьютера осуществляется автоматическое раскодирование содержимого boot-секторов защищенных логических разделов при обращении к ним.

Выбор логических разделов, для которых устанавливается режим защиты (то есть модифицируются boot-секторы), осуществляет администратор.

Механизм защиты дисков может использоваться при условии, если физический диск, с которого выполняется загрузка ОС, относится к одному из следующих типов:

- диск с таблицей разделов на идентификаторах GUID (GUID Partition Table — GPT) на компьютере с интерфейсом UEFI. При включении механизма на диск записывается специальный загрузчик Secret Net Studio в скрытом системном UEFI-разделе, после чего загрузчик регистрируется в UEFI;
- диск с основной загрузочной записью MBR. При включении механизма на этом диске модифицируется MBR и часть остального пространства нулевой дорожки диска.

Внимание! При использовании диска с основной загрузочной записью в настройках BIOS компьютера должна быть отключена функция проверки загрузочного сектора на наличие вирусов. Для отключения функции установите значение "Disabled" для параметра "Boot Virus Detection" (наличие данной функции и название параметра зависит от используемой версии BIOS).

При работе механизма обеспечивается защита до 128 логических разделов при общем количестве физических дисков до 32. Логические разделы, для которых устанавливается режим защиты, должны иметь файловую систему FAT, NTFS или ReFS. Разделы могут быть на физических дисках с основной загрузочной записью (MBR) или с таблицей разделов на идентификаторах GUID (GPT). Диски с другими типами разбиения на логические разделы не поддерживаются (например, динамические диски).

При использовании механизма защиты дисков на компьютере должна быть установлена только одна ОС. Если установлено несколько ОС, после включения механизма в одной из них не гарантируется устойчивая работа остальных ОС.

Внимание!

- Зашифрованный раздел жесткого диска невозможно поставить на защиту с помощью механизма защиты диска Secret Net Studio. И наоборот, защищенный раздел жесткого диска невозможно зашифровать с помощью механизма полнодискового шифрования Secret Net Studio.
- Не поддерживается одновременное функционирование механизмов защиты диска и доверенной среды Secret Net Studio.
- Не поддерживается корректное функционирование механизма защиты дисков, если на системном диске со структурой разделов MBR имеется раздел с EFI-загрузчиком.

Шифрование данных на дисках

Механизм полнодискового шифрования Secret Net Studio позволяет шифровать данные на носителях информации для предотвращения попыток несанкционированного доступа к конфиденциальной информации, хранящейся на этих носителях.

Поддерживается шифрование системных и несистемных разделов жестких дисков со структурой разделов GPT и режимом загрузки UEFI, а также шифрование несистемных разделов жестких дисков со структурой разделов MBR.

Максимальное количество зашифрованных разделов на одном жестком диске — 32. Количество жестких дисков не ограничено. Максимальное полное количество зашифрованных разделов на всех жестких дисках — 66.

Пояснение. В указанные ограничения также входят разделы, защищенные с помощью механизма защиты диска Secret Net Studio.

Шифрование выполняется по алгоритму AES-256. Ключевая информация хранится в зашифрованном виде на незашифрованном разделе ESP (EFI System Partition).

Для получения доступа к зашифрованным дискам необходим пароль, установленный при шифровании данных. Шифрование нескольких дисков осуществляется с одним паролем доступа.

Подсистема полнодискового шифрования Secret Net Studio предоставляет следующие возможности:

- **Локальное шифрование данных пользователем с локальным хранением данных восстановления**. Данный режим позволяет пользователю шифровать данные на дисках на компьютере с Secret Net Studio в автономном или сетевом режиме функционирования. Пользователь выбирает диски и разделы, устанавливает пароль, сохраняет данные восстановления.

  Возможность расшифрования и восстановления данных имеется только у пользователя.

  Для предоставления пользователю возможности шифрования данных на дисках администратор безопасности назначает ему соответствующую привилегию в Secret Net Studio с настройкой, что пользователь самостоятельно сохраняет данные восстановления.

- **Локальное шифрование данных пользователем с централизованным хранением данных восстановления**. Данный режим позволяет пользователю шифровать данные на дисках на компьютере с Secret Net Studio в сетевом режиме функционирования. Пользователь выбирает диски и разделы, устанавливает пароль. Данные восстановления сохраняются в централизованном хранилище Secret Net Studio.

  Возможность расшифрования и восстановления данных имеется у пользователя и администратора.

  Для предоставления пользователю возможности шифрования данных на дисках администратор безопасности назначает ему соответствующую привилегию в Secret Net Studio с настройкой, что данные восстановления должны храниться централизованно.

- **Локальное шифрование данных администратором**. В данном режиме администратор осуществляет шифрование определенного раздела локального жесткого диска компьютера с Secret Net Studio в автономном или сетевом режиме функционирования. Администратор выбирает раздел, устанавливает временный пароль, включая параметр смены пароля после первого входа в систему и сохраняет данные восстановления. Администратор передает пользователю временный пароль. Пользователь устанавливает свой пароль при первом входе в систему.

  Возможность расшифрования и восстановления данных имеется только у администратора.

- **Централизованное шифрование данных администратором**. В данном режиме администратор осуществляет шифрование определенных носителей или разделов на группе компьютеров с Secret Net Studio в сетевом режиме функционирования. Администратор выбирает носители или типы разделов для шифрования (системные, несистемные или все). Пользователь устанавливает пароль. Данные восстановления сохраняются в централизованном хранилище Secret Net Studio.

  Возможность расшифрования и восстановления данных имеется только у администратора.

При включении подсистемы полнодискового шифрования на компьютер устанавливается загрузчик Secret Net Studio. Если на компьютере имеются зашифрованные диски, при включении компьютера стартует загрузчик Secret Net Studio и запрашивается пароль доступа к дискам.

В Secret Net Studio осуществляется мониторинг и аудит процессов шифрования. Администратор может просмотреть текущее состояние подсистемы полнодискового шифрования в Центре управления или в Локальном центре управления. События подсистемы полнодискового шифрования регистрируются в журнале Secret Net Studio. На компьютере с функционирующей подсистемой появляются уведомления об основных процессах шифрования.

Имеются инструменты для восстановления доступа при потере пароля доступа к зашифрованным дискам или выходе компьютера из строя:

- если у пользователя имеются данные восстановления, при входе в систему можно ввести код восстановления и пароль к коду восстановления, а также сменить пароль доступа к дискам;
- если пользователь осуществлял шифрование и данные восстановления хранятся в централизованном хранилище, администратор высылает пользователю код восстановления и пользователь меняет пароль доступа к дискам;
- если компьютер с зашифрованными данными вышел из строя, осуществляется загрузка с диска аварийного восстановления для восстановления конфигурации зашифрованных разделов или расшифрования данных.

Данные восстановления шифруются с помощью ключа домена безопасности Secret Net Studio. Ключ домена безопасности создается при создании домена или обновлении сервера безопасности и может быть обновлен администратором домена безопасности.

Для использования подсистемы полнодискового шифрования Secret Net Studio необходима отдельная лицензия. По истечении срока действия лицензии возможен доступ к зашифрованным данным, а также доступны операции расшифрования и восстановления доступа.

Внимание!

- Зашифрованный раздел жесткого диска невозможно поставить на защиту с помощью механизма защиты диска Secret Net Studio. И наоборот, защищенный раздел жесткого диска невозможно зашифровать с помощью механизма полнодискового шифрования Secret Net Studio.
- Не поддерживается одновременное функционирование механизмов полнодискового шифрования и доверенной среды Secret Net Studio.
- Не поддерживается функционирование механизма полнодискового шифрования на компьютере с несколькими ОС.
- Не поддерживается корректное функционирование механизма полнодискового шифрования, если на системном диске со структурой разделов MBR имеется раздел с EFI-загрузчиком.
- Не поддерживается шифрование динамических дисков.
- Не поддерживается изменение конфигурации зашифрованных разделов жестких дисков (перераспределение жесткого диска и др.).
- Не поддерживается параллельная работа с другими системами шифрования дисков (например, Bitlocker).

Шифрование данных в криптоконтейнерах

Система Secret Net Studio предоставляет возможность шифрования содержимого объектов файловой системы (файлов и папок). Для операций зашифрования и расшифрования используются специальные хранилища — криптографические контейнеры или криптоконтейнеры.

Физически криптоконтейнер представляет собой файл, который можно подключить к системе в качестве дополнительного диска. Криптоконтейнер является образом диска, но все действия с ним выполняются через драйвер механизма шифрования. Драйвер обеспечивает работу с пользовательскими данными в контейнере в режиме "прозрачного шифрования". То есть пользователь, после подключения криптоконтейнера в качестве диска, выполняет операции с файлами на этом диске так же, как и на любом другом носителе. Дополнительных действий для зашифрования или расшифрования файлов не требуется. Все криптографические операции с файлами выполняются автоматически.

Криптоконтейнеры можно подключать к системе с локальных дисков, сменных носителей или с сетевых ресурсов. Доступный объем для записи данных указывается при создании криптоконтейнера. Предельное ограничение объема определяется исходя из свободного пространства на ресурсе и типа файловой системы. Минимальный размер контейнера — 1 Мбайт.

Для разграничения доступа пользователей к криптоконтейнерам в системе Secret Net Studio предусмотрены следующие права:

- чтение данных — предоставляет только возможности чтения файлов в криптоконтейнере;
- полный доступ к данным — предоставляет возможности чтения и записи файлов в криптоконтейнере;
- управление криптоконтейнером — предоставляет возможности управления списком пользователей, имеющих доступ к криптоконтейнеру, а также чтения и записи файлов.

Создание криптоконтейнеров доступно пользователям с соответствующей привилегией. По умолчанию эта привилегия предоставлена всем учетным записям, которые входят в локальные группы администраторов или пользователей.

Пользователь, создавший криптоконтейнер, получает право на управление им и в дальнейшем может делегировать (предоставить) это право доступа другому пользователю. При необходимости создатель криптоконтейнера может быть удален из списка пользователей с правами доступа с тем условием, что в списке будет присутствовать хотя бы один пользователь с правами на управление криптоконтейнером.

Для работы с шифрованными ресурсами пользователи должны иметь ключи шифрования. Процедуры генерации и выдачи ключей выполняются администратором безопасности. Для пользователей создаются ключевые пары, каждая из которых состоит из открытого и закрытого ключей. Открытые ключи хранятся в общем хранилище (для ключей локальных пользователей используется локальная БД Secret Net Studio, для доменных — хранилище глобального каталога). Закрытые ключи хранятся в ключевых носителях, присвоенных пользователям. Носителями для хранения закрытых ключей (ключевой информации) могут являться идентификаторы или сменные носители, такие как флеш-карты, флеш-накопители и т. п.

Общие сведения о ключевой схеме

Реализация ключевой схемы шифрования криптоконтейнеров базируется на алгоритмах ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 и ГОСТ 28147–89. Во время криптографических операций генерируются и вычисляются определенные наборы ключей и дополнительных значений, используемых для доступа к криптоконтейнеру.

Криптоконтейнер содержит следующие группы данных:

- управляющая информация криптоконтейнера — представляет собой структуру зашифрованных ключей и значений для доступа к криптоконтейнеру;
- зашифрованные данные пользователей — криптографически преобразованные файлы, помещенные в криптоконтейнер пользователями.

Управляющая информация криптоконтейнера формируется при его создании. Изначально в этой структуре совместно с другими сведениями сохраняется открытый ключ пользователя, создавшего криптоконтейнер. Далее в процессе формирования списка пользователей, имеющих доступ к контейнеру, открытые ключи этих пользователей также помещаются в структуру. С использованием открытых ключей шифруются соответствующие части структуры.

Файлы, помещаемые пользователями в криптоконтейнер, шифруются с использованием ключей шифрования, рассчитанных на основе базового ключа шифрования — общего для всех пользователей криптоконтейнера. Базовый ключ шифрования генерируется при создании криптоконтейнера. Вычисление ключа осуществляется при доступе к криптоконтейнеру с помощью закрытого ключа пользователя.

Для дополнительной защиты базового ключа шифрования может использоваться специальный "корпоративный ключ". Данный ключ генерируется при создании криптоконтейнера, если включен параметр "использовать корпоративный ключ". Ключ сохраняется в системном реестре компьютера и применяется для зашифрования и расшифрования базового ключа.

При использовании корпоративного ключа доступ к криптоконтейнеру возможен при условии, если ключ хранится в системном реестре (в зашифрованном виде). Поэтому для доступа к криптоконтейнеру на другом компьютере корпоративный ключ необходимо импортировать в реестр этого компьютера.

Смена ключей

В процессе эксплуатации системы следует регулярно выполнять смену ключей пользователей и базовых ключей шифрования криптоконтейнеров.

Смена ключей пользователя выполняется самим пользователем или администратором безопасности. Периодичность смены ключей пользователей контролируется системой и может настраиваться путем ограничения максимального и минимального сроков действия ключей. При смене ключей пользователя в системе сохраняются две ключевые пары — текущая и предыдущая. Предыдущая ключевая пара необходима для перешифрования на новом ключе соответствующей части управляющей информации в криптоконтейнерах пользователя. Процесс перешифрования управляющей информации запускается автоматически после смены ключей.

Внимание! Автоматическое перешифрование управляющей информации возможно при условии доступности криптоконтейнера. Например, если криптоконтейнер недоступен по сети или находится на сменном носителе, который не подключен в данный момент, — перешифрование не происходит. В этом случае после смены ключей для перешифрования управляющей информации пользователю необходимо выполнить какую-либо операцию с таким криптоконтейнером (например, подключить криптоконтейнер) до следующей смены ключей. Иначе во время следующей смены будет заменена предыдущая ключевая пара, и пользователь не сможет получить доступ к криптоконтейнеру из-за несовпадения ключей. Для возобновления доступа потребуется удалить пользователя из списка имеющих доступ к криптоконтейнеру и затем снова добавить в этот список.

Смена базового ключа шифрования криптоконтейнера выполняется пользователем с правами на управление криптоконтейнером. Для смены базового ключа пользователь инициирует процедуру перешифрования криптоконтейнера, в результате чего все зашифрованные данные криптоконтейнера будут перешифрованы на новом базовом ключе. При использовании корпоративного ключа его смена происходит автоматически при смене базового ключа.

Паспорт ПО

Механизм "Паспорт ПО" предназначен для контроля состава и целостности ПО, установленного на защищаемых компьютерах. Контроль ПО осуществляется посредством сканирования исполняемых файлов и расчета их контрольных сумм. Совокупность контролируемых файлов на дисках компьютера представляет программную среду для сбора данных и анализа изменений.

Распознавание исполняемых файлов осуществляется по расширениям имен. Перечень расширений и каталоги поиска файлов можно настраивать. Сканирование выполняется периодически по расписанию или в произвольные моменты времени по команде пользователя.

После сканирования полученные данные о состоянии программной среды защищаемого компьютера загружаются на сервер безопасности и получают статус проекта паспорта для компьютера. Эти данные сравниваются с результатами предыдущего сканирования, которые хранятся в виде утвержденного паспорта. Изменения анализируются, и при необходимости проект паспорта утверждается в качестве текущего паспорта защищаемого компьютера.

Доверенная среда

Доверенная среда Secret Net Studio является механизмом защиты, обеспечивающим внешний по отношению к ОС контроль работы ОС и системы защиты, установленных на компьютере. Контроль достигается выполнением следующих функций безопасности:

- контроль целостности модулей Secret Net Studio (драйверов, служб, приложений);
- контроль запуска и функционирования модулей Secret Net Studio (драйверов, служб, приложений);
- блокировка от записи страниц памяти, в которых размещаются модули Secret Net Studio;
- обнаружение компьютерных атак, их предотвращение или аварийное завершение работы ОС компьютера при невозможности предотвращения атаки;
- регистрация событий в журнале ДС.

При функционирующей ДС загрузка ОС компьютера осуществляется с использованием загрузочного носителя, подготовленного заранее средствами Secret Net Studio.

Примечание.
- ДС доступна в Secret Net Studio версии 8.5 и выше.
- Не поддерживается одновременное функционирование доверенной среды и механизма полнодискового шифрования Secret Net Studio.

Безопасная среда

Безопасная среда является механизмом защиты, позволяющим предотвратить нанесение ущерба ресурсам защищаемого компьютера путем запуска неизвестного программного обеспечения в изолированной среде. Запуск неизвестного ПО может выполняться пользователями и администраторами.

При взаимодействии пользователя с проверяемым ПО Безопасная среда осуществляет мониторинг и анализ производимых действий:

Если поведение ПО отличается от приемлемого, Безопасная среда принудительно завершает работу программы, вносит ее в список заблокированных (черный список) и оповещает пользователя об осуществленных действиях.

Если поведение ПО не является подозрительным и достигает указанного в ПУ уровня доверия, Безопасная среда вносит его в перечень доверенных программ.

Если пользователь заканчивает работу программы раньше окончания ее проверки, Безопасная среда сохраняет контекст анализа программы и использует его при следующем запуске программы в Безопасной среде.

Примечание. Безопасная среда доступна в Secret Net Studio версии 8.7 и выше.

Межсетевой экран

Secret Net Studio обеспечивает контроль сетевого трафика на сетевом, транспортном и прикладном уровнях на основе формируемых правил фильтрации.

Подсистема межсетевого экранирования Secret Net Studio реализует следующие основные функции:

- фильтрация на сетевом уровне с независимым принятием решений по каждому пакету;
- фильтрация пакетов служебных протоколов (ICMP, IGMP и т.д.), необходимых для диагностики и управления работой сетевых устройств;
- фильтрация с учетом входного и выходного сетевого интерфейса для проверки подлинности сетевых адресов;
- фильтрация на транспортном уровне запросов на установление виртуальных соединений (TCP-сессий);
- фильтрация на прикладном уровне запросов к прикладным сервисам (фильтрация по символьной последовательности в пакетах);
- фильтрация с учетом полей сетевых пакетов;
- фильтрация с учетом даты/времени суток.

Фильтрация сетевого трафика осуществляется на интерфейсах Ethernet (IEEE 802.3) и Wi-Fi (IEEE 802.11b/g/n). События, связанные с работой межсетевого экрана, регистрируются в журнале Secret Net Studio.

Авторизация сетевых соединений

При действующем механизме авторизации сетевых соединений осуществляется добавление специальной служебной информации к сетевым пакетам, с помощью которой обеспечивается аутентичность и целостность передаваемых данных и защита от атак типа Man in the Middle.

Подсистема авторизации сетевых соединений обеспечивает:

- получение с сервера авторизации, входящего в состав компонента "Secret Net Studio — Сервер безопасности", правил авторизации соединений (список параметров соединений, в которые добавляется служебная информация);
- получение с сервера авторизации сессионных данных для добавления служебной информации;
- добавление в сетевой трафик специальной служебной информации для пакетов, удовлетворяющих правилам авторизации;
- разбор специальной служебной информации во входящих пакетах и передачу информации о контексте удаленного пользователя в подсистему межсетевого экранирования для фильтрации по правилам.

Авторизация сетевых соединений осуществляется на интерфейсах Ethernet (IEEE 802.3) и Wi-Fi (IEEE 802.11b/g/n).

Глава 4
Общие сведения о централизованном управлении

Взаимодействующие компоненты

Сервер безопасности

Основные функции сервера безопасности:

- получение информации от агентов на защищаемых компьютерах о текущем состоянии рабочих станций и сессиях работы пользователей;
- оперативное получение и передача сведений о событиях тревоги, зарегистрированных на защищаемых компьютерах;
- отправка команд управления на защищаемые компьютеры;
- получение информации о состоянии защитных подсистем на компьютерах и отправка команд на изменение состояния защитных подсистем;
- получение и передача на защищаемые компьютеры параметров групповых политик, заданных в Центре управления Secret Net Studio;
- контроль действительности лицензий на использование компонентов системы Secret Net Studio;
- получение локальных журналов с защищаемых компьютеров и передача содержимого журналов в базу данных сервера безопасности;
- обработка запросов к базе данных;
- архивирование и восстановление содержимого журналов в базе данных;
- протоколирование обращений к серверу.

Сервер безопасности реализует функции контроля и управления защищаемыми компьютерами при условии их подчинения. Серверу могут быть подчинены компьютеры с установленным клиентом Secret Net Studio, компьютеры под управлением ОС семейства Linux с установленным ПО Secret Net LSP, а также другие серверы безопасности.

Внимание! Для компьютеров под управлением ОС семейства Linux с установленным ПО Secret Net LSP и для подчиненных серверов безопасности некоторые функции сервера недоступны (см. стр.44 и стр.42 соответственно).

Для функционирования сервера безопасности требуется наличие СУБД, реализуемой сервером СУБД MS SQL. Сервер безопасности и сервер СУБД могут быть установлены на разных компьютерах (рекомендуется) или на одном компьютере.

Сервер авторизации

В состав ПО сервера безопасности входит отдельное приложение — сервер авторизации. Данное приложение обеспечивает работу механизмов межсетевого экрана и авторизации сетевых соединений. Сервер авторизации устанавливается и удаляется вместе с ПО сервера безопасности.

Шлюз

В состав ПО сервера безопасности также входит отдельный компонент — шлюз. Шлюз является службой, которая обеспечивает взаимодействие двух серверов безопасности, находящихся в разных и несвязанных лесах доменов AD. Один из них является родительским или корневым по отношению к другому. Взаимодействие состоит в передаче данных о функционировании агентов сервером из дочернего домена AD корневому серверу и передаче информации о политиках безопасности с коревого сервера в дочерний лес доменов AD. Также есть возможность на корневом сервере выполнять управление агентами из другого леса AD.

Центр управления

Центр управления устанавливается на рабочих местах администраторов и используется для централизованного управления защищаемыми компьютерами. Программа осуществляет взаимодействие с сервером безопасности, через который выполняются необходимые действия.

Клиент в сетевом режиме функционирования

Для реализации централизованного управления на всех защищаемых компьютерах должен быть установлен клиент Secret Net Studio в сетевом режиме функционирования. Эти компьютеры необходимо подчинить серверам безопасности.

Сетевая структура Secret Net Studio

Домены безопасности

В системе Secret Net Studio реализация централизованного управления компьютерами и синхронизации параметров защиты базируется на концепции доменов безопасности. Домены безопасности формируются из объектов, включенных в определенные контейнеры Active Directory — организационные подразделения (Organizational Unit) или весь домен AD.

Формирование домена безопасности в домене AD происходит при установке сервера безопасности.

Сетевая структура системы Secret Net Studio строится по принципу подчинения защищаемых компьютеров сети серверу безопасности. Для подчинения серверу безопасности компьютер должен быть в составе домена безопасности.

Сервер безопасности использует базу данных служб облегченного доступа к каталогам Active Directory (Active Directory Lightweight Directory Services, AD LDS). Контроль получения и применения параметров на защищаемых компьютерах осуществляется самим сервером безопасности.

При создании домена безопасности назначается группа пользователей, которым будут предоставлены права администрирования домена безопасности, — группа администраторов домена безопасности.

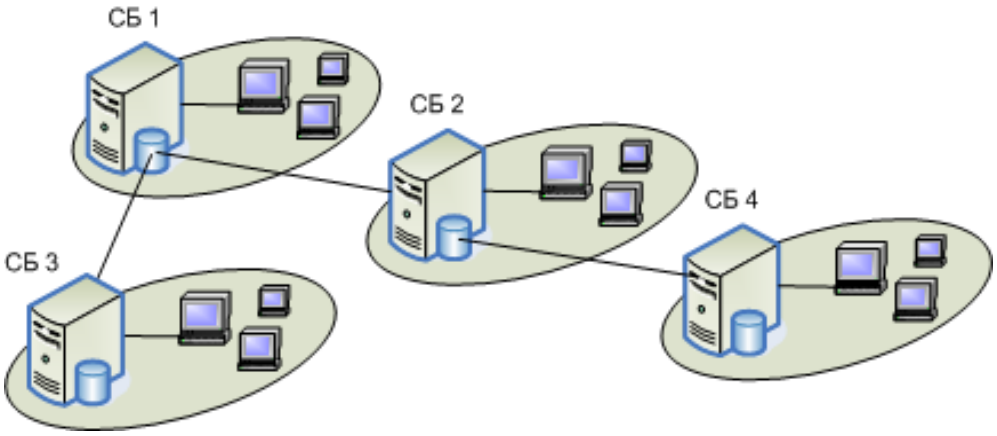
Внимание! Чтобы обеспечить бесперебойное функционирование защищаемых компьютеров, следует предусмотреть наличие в домене безопасности постоянно работающего резервного сервера безопасности.

Леса доменов безопасности

По аналогии с доменами Active Directory несколько доменов безопасности (со своими серверами безопасности) могут образовывать лес доменов.

Для леса назначается группа пользователей, которым будут предоставлены права на создание новых доменов безопасности. Эта группа будет являться группой администраторов леса доменов безопасности.

В рамках леса доменов можно организовать функционирование нескольких серверов безопасности с подчинением по иерархическому принципу. При этом иерархия подчинения серверов не обязательно должна соответствовать структуре доменов в лесу. На рисунке представлен пример использования нескольких серверов СБ1 — СБ4.



Каждый сервер контролирует работу своей группы защищаемых компьютеров и имеет свою базу данных. При этом некоторые операции доступны и в отношении объектов, относящихся к подчиненным серверам. Как видно из рисунка, серверы безопасности СБ2 и СБ3 являются подчиненными по отношению к СБ1, а СБ4 — подчиненным по отношению к СБ2.

Федерация

Система Secret Net Studio позволяет организовать иерархическую структуру лесов доменов безопасности на основе несвязанных лесов доменов Windows AD. Под последними понимаются отдельные леса доменов Windows AD, между которыми не установлены доверительные отношения.

В этом случае один из лесов доменов безопасности Secret Net Studio становится корневым или родительским, а остальные леса безопасности становятся по отношению к нему подчиненными или дочерними.

Для взаимодействия лесов безопасности используется специальный шлюз. Шлюз размещается в каждом из дочерних лесов безопасности. Все они регистрируются на родительском сервере безопасности. Все леса безопасности, относящиеся к данному серверу, формируют единое объединение, называемое федерацией.

Для синхронизации данных между лесами AD вводится отдельная служба. Служба синхронизации устанавливается на стороне дочернего сервера. Служба развертывается отдельным установщиком, который встроен в процесс установки сервера безопасности.

После такого объединения администратору, работающему с родительским сервером безопасности, предоставляются следующие возможности по управлению защищаемыми компьютерами из дочерних лесов безопасности:

- получение информации о состоянии защищаемых компьютеров;
- отправка команд оперативного управления на защищаемые компьютеры;
- получение оповещений о событиях тревоги и сбор локальных журналов с защищаемых компьютеров;
- управление параметрами безопасности этих компьютеров посредством групповых политик, заданных на родительском сервере безопасности.

В рамках сетевой структуры можно организовать функционирование нескольких лесов безопасности с подчинением по иерархическому принципу. На рисунке представлен пример, иллюстрирующий подчинение одного леса безопасности другому.

В каждом лесу имеется своя иерархия серверов безопасности. На сервере СБ1b установлен шлюз, связывающий этот дочерний сервер с родительским сервером СБ1. При работе с родительским сервером СБ1 администратору безопасности будет доступно управление как всеми серверами и защищаемыми компьютерами родительского леса, так и всеми серверами и защищаемыми компьютерами дочернего леса (в ограниченном объеме перечисленных выше возможностей).

Ограничения

При планировании и развертывании подобной сетевой структуры необходимо учитывать следующие ограничения ее использования:

- для взаимодействия двух лесов безопасности можно использовать только один шлюз. Второй шлюз в данной паре лесов установить нельзя;
- поддерживается только двухуровневая иерархия лесов безопасности. Это означает, что дочернему лесу безопасности нельзя подчинить еще один дочерний лес безопасности.

Особенности формирования сетевой структуры

Сетевую структуру системы Secret Net Studio можно формировать с учетом различных особенностей построения сети и распределения полномочий между администраторами. Одним из основных факторов, влияющих на формирование сетевой структуры системы Secret Net Studio, является вопрос наделения полномочиями администраторов безопасности. При необходимости разделить полномочия администраторов следует сформировать домены безопасности на базе организационных подразделений. Такой вариант позволяет в нужном объеме разделить полномочия администраторов безопасности и администраторов домена Active Directory, поскольку в рамках организационного подразделения администратору безопасности могут быть предоставлены все необходимые права на администрирование.

В один лес безопасности, независимо от количества серверов безопасности в нем, рекомендуется включать не более 15 000 функционирующих клиентов. Одному серверу безопасности рекомендуется подчинять не более 1 500 функционирующих клиентов. Рекомендуемое количество может варьироваться в зависимости от конфигурации леса безопасности и домена AD (настройки сборки журналов, политик, количества контролируемых устройств, количества учетных записей пользователей и др.).

Обмен данными между клиентами и сервером осуществляется в режиме сессий. При передаче данных используется протокол HTTPS. На сервере должен быть установлен сертификат для обеспечения защиты соединений с сервером.

Управление компьютерами с СЗИ Secret Net LSP

В Secret Net Studio имеется возможность централизованного управления, мониторинга и получения локальных журналов для компьютеров, функционирующих под управлением ОС семейства Linux. Для этого на компьютерах должно быть установлено средство защиты информации Secret Net LSP (версии 1.7 и выше) и выполнена настройка удаленного управления. Описание последовательности действий для настройки удаленного управления в Secret Net LSP см. в документации на этот продукт.

Управление доменными пользователями

Настройка параметров доменных пользователей для работы в системе Secret Net Studio осуществляется в Центре управления пользователями. Программа входит в состав средств управления Secret Net Studio и дополнительно предоставляет возможности создания и удаления учетных записей, а также позволяет настраивать основные параметры пользователей и групп.

Штатные средства ОС (оснастки для управления пользователями) рекомендуется использовать только для настройки параметров, отсутствующих в Центре управления пользователями. При создании или удалении учетных записей с использованием штатных средств некоторые функции управления и контроля могут быть недоступны до синхронизации изменений в системе Secret Net Studio.

Централизованное хранение данных

Компоненты системы Secret Net Studio используют следующие структуры централизованного хранения данных:

- база данных сервера безопасности на сервере СУБД — содержит централизованные журналы и оперативную информацию для мониторинга системы;
- база данных служб AD LDS — содержит параметры системы Secret Net Studio, относящиеся к учетным записям, списки серверов безопасности, списки электронных идентификаторов и других объектов для централизованного управления системой защиты.

Разделение хранилищ обусловлено спецификой обращения к данным. Обращения осуществляют только те компоненты, которым это разрешено. Контроль и разграничение доступа к хранилищам осуществляются самой системой, поэтому от администратора не требуется дополнительных действий для обеспечения защиты обращений.

Глава 5
Развертывание Secret Net Studio

Структура системы Secret Net Studio является модульной. Подробные сведения об архитектуре системы Secret Net Studio содержатся в предыдущих главах данного документа.

Состав устанавливаемых компонентов

Система Secret Net Studio состоит из следующих программных пакетов, устанавливаемых на компьютерах:

1. "Secret Net Studio" (далее — клиент).
2. "Secret Net Studio — Сервер безопасности" (далее — сервер безопасности или СБ).
3. "Secret Net Studio — Центр управления" (далее — Центр управления).

Требования к аппаратному и программному обеспечению

Клиент

Компонент "Secret Net Studio" устанавливается на компьютеры, работающие под управлением следующих ОС (поддерживаются 32- и 64-разрядные версии ОС с установленными пакетами обновлений не ниже указанных):

- Windows 11;
- Windows 10;
- Windows 8.1 Rollup Update;
- Windows 7 SP1 KB3033929 (при наличии купленной поддержки производителя);
- Windows Server 2019;
- Windows Server 2016;
- Windows Server 2012 R2 Rollup Update;
- Windows Server 2008 R2 SP1 KB3033929 (при наличии купленной поддержки производителя).

Внимание! Во избежание конфликтов средств защиты необходимо до установки Secret Net Studio убедиться в отсутствии на защищаемых компьютерах других установленных средств защиты информации от несанкционированного доступа, межсетевых экранов.

Для установки клиента в сетевом режиме функционирования компьютер должен быть включен в домен Active Directory.

Требования к аппаратной конфигурации компьютера:

Элемент	Минимально
Процессор	В соответствии с требованиями ОС
Оперативная память	2 ГБ
Жесткий диск (свободное пространство)	4 ГБ

Внимание!

- Для использования доверенной среды компьютер должен удовлетворять требованиям, указанным в документе [**2**], глава "Доверенная среда".
- Для использования подсистемы полнодискового шифрования на компьютере должен быть установлен режим загрузки UEFI.

Системный каталог ОС Windows %SystemRoot% должен располагаться на томе с файловой системой NTFS или NTFS5.

Для установки клиента на компьютере должно быть установлено следующее ПО:

- Internet Explorer версии 8 или выше.

Если на компьютере будут использоваться аппаратные средства защиты (ПАК "Соболь" или другие поддерживаемые средства), рекомендуется выполнить подготовку устройств к использованию до установки клиентского ПО системы Secret Net Studio. Действия для подготовки устройств выполняются в соответствии с документацией на изделие. Установку ПО для поддерживаемых USB-ключей и смарт-карт можно выполнять с установочного диска системы Secret Net Studio. Файлы для установки расположены в соответствующих подкаталогах каталога \Tools\ (сведения о размещении файлов см. в приложении на стр.**271**).

Установка клиента в сетевом режиме функционирования может выполняться централизованно под управлением сервера безопасности. В этом случае необходимо настроить следующее:

- В брандмауэре, если он включен, необходимо разрешить использование портов для доступа к общим ресурсам: UDP –137, 138; TCP – 139, 445. Данные порты по умолчанию закрыты брандмауэром при отсутствии на компьютере сетевых папок общего доступа.
- Должны быть открыты все TCP, UDP-порты, необходимые для функционирования компонентов ОС Windows в домене AD.
- Должен быть настроен доступ к системным общим ресурсам ADMIN$ и IPC$. Для этого необходимо разрешить использование портов для доступа к общим ресурсам (см. выше), а также обеспечить возможность удаленного входа на компьютер под учетной записью, которая была указана в задании централизованного развертывания.

Пояснение. Список всех портов, которые должны быть открыты для корректного функционирования Secret Net Studio, приведены на стр.**269**.

Программа установки клиента до начала модификации системы автоматически создает точку восстановления ОС. В процессе установки проверяются и при необходимости автоматически устанавливаются следующие распространяемые пакеты компании Microsoft:

- Microsoft Visual C++ 2015-2019 Redistributable - 14.28.29325;
- Microsoft .NET Framework 4.5;
- пакет обновлений KB2462317;
- службы Microsoft Core XML Services (MSXML) 6.0;
- Microsoft XML Paper Specification Essentials Pack (пакет XPS EP).

После установки обновлений может потребоваться перезагрузка компьютера.

Сервер безопасности

Компонент "Secret Net Studio — Сервер безопасности" устанавливается на компьютеры, включенные в домен Active Directory и работающие под управлением следующих ОС:

- Windows Server 2022;
- Windows Server 2019;
- Windows Server 2016;
- Windows Server 2012 R2 Rollup Update;
- Windows Server 2008 x64 R2 SP1 KB3033929 (при наличии купленной поддержки производителя).

Требования к аппаратной конфигурации компьютера:

Элемент	Минимально	Рекомендуется
Процессор	В соответствии с требованиями ОС	Intel Core i5/Xeon E3 и выше
Оперативная память	8 ГБ	16 ГБ[1]

Элемент	Минимально	Рекомендуется
Жесткий диск (свободное место)	150 ГБ Рекомендуется использовать высокоскоростной жесткий диск	

[1] При размещении СБ и сервера СУБД на одном компьютере.

Для функционирования компонента требуется наличие системы управления базами данных, реализуемой сервером СУБД MS SQL. Сервер безопасности и сервер СУБД могут быть установлены на разных компьютерах (рекомендуется) или на одном компьютере.

Версии программного обеспечения серверов баз данных, совместимые с сервером безопасности (поддерживаются 32- и 64-разрядные версии, включая свободно распространяемые варианты SQL Server Express):

- Microsoft SQL Server 2019;
- Microsoft SQL Server 2017;
- Microsoft SQL Server 2016;
- Microsoft SQL Server 2014;
- Microsoft SQL Server 2012 с пакетом обновления 1 (SP1) и выше;
- Microsoft SQL Server 2008 R2 с пакетом обновления 1 (SP1) и выше.

Пояснение. Корректное взаимодействие сервера безопасности и СУБД MS SQL обеспечивается при выполнении условий, изложенных в приложении на стр.272.

Дополнительно к компьютеру предъявляются следующие требования:

- на компьютере должны быть свободны и открыты TCP-порты 50000–50003. Если эти порты заняты другими приложениями, при установке сервера безопасности будет предложено выбрать другие порты для использования службами каталогов. Кроме того, должны быть открыты все TCP, UDP-порты, необходимые для функционирования компонентов ОС Windows в домене AD;

  Пояснение. Список всех портов, которые должны быть открыты для корректного функционирования Secret Net Studio, приведены на стр.269.

- в качестве языка программ, не поддерживающих стандарт кодирования Юникод, должен быть указан русский язык.

Программа установки автоматически проверяет и при необходимости устанавливает следующий распространяемый пакет компании Microsoft:

- Microsoft Visual C++ 2015-2019 Redistributable.

После установки обновлений может потребоваться перезагрузка компьютера.

Центр управления

Компонент "Secret Net Studio — Центр управления" устанавливается на компьютеры, включенные в домен Active Directory и работающие под управлением следующих ОС (поддерживаются 32- и 64-разрядные версии ОС с установленными пакетами обновлений не ниже указанных):

- Windows 11;
- Windows 10;
- Windows 8.1 Rollup Update;
- Windows 7 SP1 KB3033929 (при наличии купленной поддержки производителя);
- Windows Server 2022;
- Windows Server 2019;
- Windows Server 2016;
- Windows Server 2012 R2 Rollup Update;
- Windows Server 2008 x64 R2 SP1 KB3033929 (при наличии купленной поддержки производителя).

Требования к аппаратной конфигурации компьютера:

Элемент	Минимально
Процессор	В соответствии с требованиями ОС
Оперативная память	2 ГБ[1]
Жесткий диск (свободное пространство)	4 ГБ[2]

[1] При работе с журналами указанный объем памяти является достаточным для отображения до 1—1,5 млн записей. Чтобы загружать больше данных (например, для просмотра архивов размером более 100 МБ), необходимо либо увеличить объем памяти, либо использовать фильтрацию записей.

[2] При работе с архивами журналов указанный объем памяти является достаточным для распаковки архивов до 80—100 МБ (разархивирование осуществляется в папке временных файлов пользователя). Чтобы загружать более объемные архивы, необходимо увеличить свободное пространство на диске, который используется для временных файлов. Например, для работы с архивами размером 200–300 МБ требуется не менее 10 ГБ свободного пространства.

Для установки Центра управления на компьютере должно быть установлено следующее ПО:

- Internet Explorer версии 8 или выше.

Программа установки также проверяет и при необходимости устанавливает в автоматическом режиме пакет Microsoft .NET Framework 4.5.

Установочный комплект системы

Программное обеспечение и эксплуатационная документация системы Secret Net Studio поставляются в виде установочного комплекта на компакт-диске или в электронном виде (далее — установочный диск, установочный комплект). В корневом каталоге диска размещается исполняемый файл программы для работы с диском (далее — программа автозапуска). Общая структура каталогов диска представлена в следующей таблице.

Каталог	Содержимое
\Setup\Server\	Дистрибутив сервера безопасности
\Setup\Console\	Дистрибутивы Центра управления
\Setup\Client\	Дистрибутивы клиента
\Documentation\	Комплект документации
\Tools\	Вспомогательные утилиты, файлы для установки и настройки ПО

Программа автозапуска

При вставке установочного диска в привод для чтения оптических дисков происходит автоматический запуск программы автозапуска, которая позволяет выполнять следующие действия:

- запускать программы установки компонентов системы Secret Net Studio;
- открывать в отдельных окнах каталоги диска.

Примечание. Если на компьютере отключена функция автозапуска оптических дисков, автоматический запуск программы не выполняется. В этом случае для работы с программой автозапуска запустите файл SnAutoRun.exe в корневом каталоге диска.

Пример содержимого окна программы автозапуска представлен на рисунке ниже.

Окно содержит команды для выполнения действий. Назначение команд описано в следующей таблице.

Команда	Назначение
Защитные компоненты	Запуск программы установки клиента
Сервер безопасности	Запуск программы установки сервера безопасности
Центр управления	Запуск программы установки Центра управления
Сервер обновлений	Запуск программы установки сервера обновлений
Дополнительное ПО	Открытие каталога \Tools\ в отдельном окне
Документация	Открытие каталога \Documentation\ в отдельном окне
RU|EN|ES	Выбор языка для программы автозапуска и устанавливаемого ПО

Для выполнения нужного действия выберите соответствующую команду. Некоторые команды запуска могут быть недоступны из-за невозможности установки компонентов или если установка не требуется. Для просмотра сведений о причине блокировки наведите указатель на команду — через 1–2 секунды на экране появится всплывающее сообщение.

Варианты установки компонентов

Компоненты системы Secret Net Studio можно устанавливать при работе на компьютере локально или в терминальных сессиях.

Кроме того, установка клиента в сетевом режиме функционирования может выполняться централизованно.

Порядок установки для централизованного управления

Подготовительные действия

Перед установкой компонентов Secret Net Studio для централизованного управления необходимо выполнить действия по подготовке к созданию доменов безопасности и сетевой структуры. Сведения о доменах безопасности и сетевой структуре Secret Net Studio см. на стр.40.

Состав подготовительных действий:

1. Если домены безопасности будут формироваться на базе организационных подразделений, подготовьте организационные подразделения и включите в них нужные компьютеры.
2. Для каждого леса доменов безопасности создайте группу пользователей, которая будет указана в качестве группы администраторов леса. Пользователи, входящие в группу администраторов леса доменов безопасности, будут обладать правами на создание новых доменов безопасности в соответствующем лесу.
3. Создайте группы пользователей, которые будут указаны в качестве групп администраторов доменов безопасности.

Общий порядок установки компонентов

Установка компонентов Secret Net Studio выполняется в следующем порядке:

1. На компьютере, который будет использоваться в качестве корневого сервера безопасности (не подчиненного другим серверам), выполните следующие действия:
   - включите группу администраторов леса доменов безопасности и группу администраторов домена безопасности в локальную группу администраторов компьютера (в соответствии с тем, к какому домену безопасности будет относиться сервер);
   - установите ПО сервера безопасности (см. стр.**52**).
2. На других компьютерах, которые будут использоваться в качестве подчиненных серверов безопасности, выполните действия аналогично п. **1**.
3. На рабочих местах администраторов Secret Net Studio установите Центр управления (см. стр.**59**).
4. Установите клиент Secret Net Studio в сетевом режиме функционирования (см. стр. **60**) на компьютерах серверов безопасности, затем на остальных компьютерах.

Типовой сценарий развертывания

Ниже рассматривается типовой сценарий развертывания компонентов системы Secret Net Studio для случая формирования одного домена безопасности на базе организационного подразделения AD. Все защищаемые компьютеры подчиняются одному серверу безопасности.

1. С использованием средств управления объектами Active Directory создайте организационное подразделение и включите в него компьютеры, на которых будет установлено ПО системы Secret Net Studio.
2. Создайте доменные группы пользователей для администраторов леса доменов безопасности и администраторов домена безопасности. Включите в эти группы учетные записи, которые должны обладать соответствующими полномочиями.
3. На компьютере, который будет использоваться в качестве сервера безопасности, выполните следующие действия:
   - включите группу администраторов леса доменов безопасности и группу администраторов домена безопасности в локальную группу администраторов компьютера;
   - установите ПО сервера безопасности (см. стр.**52**).

   Внимание! Чтобы обеспечить бесперебойное функционирование защищаемых компьютеров, следует установить резервный сервер в этом же домене безопасности. Установка резервного сервера выполняется в варианте включения сервера в состав имеющегося домена безопасности. При установке подчините резервный сервер основному серверу домена безопасности. Описание особенностей использования резервного сервера см. в приложении на стр.**278**.
4. На компьютере администратора безопасности установите Центр управления (см. стр.**59**).

5. Запустите Центр управления и установите соединение с сервером безопасности.
6. Настройте централизованную установку клиентского ПО Secret Net Studio на компьютерах организационного подразделения. Для этого добавьте комплект установочных файлов клиента в список централизованно устанавливаемого ПО и сформируйте задания развертывания (см. стр.64).
7. Отслеживайте выполнение заданий в Центре управления. После установки клиентского ПО и перезагрузки компьютеров они будут появляться в структуре управления в качестве подчиненных объектов сервера безопасности.

Глава 6
Локальная установка компонентов

Установку компонентов Secret Net Studio можно выполнять при работе на компьютере как в локальной сессии, так и в терминальной. Установка любого компонента должна выполняться пользователем, входящим в локальную группу администраторов компьютера.

Для централизованного управления клиентами в сетевом режиме функционирования необходимо установить сервер безопасности и Центр управления. Управление клиентами в автономном режиме осуществляется только локально, поэтому установка указанных компонентов не требуется.

Установка сервера безопасности

Перед установкой сервера безопасности необходимо установить ПО сервера СУБД MS SQL (сведения о вариантах установки ПО см. на стр.**46**).

Для выполнения некоторых действий при установке сервера безопасности могут потребоваться особые права доступа. Например, права на администрирование леса доменов безопасности. Если пользователь, выполняющий установку, не обладает нужными правами, программа установки на определенных этапах может запрашивать учетные данные пользователей с правами доступа.

Внимание! После установки сервера безопасности нельзя изменять имя компьютера сервера. Если компьютер будет переименован, сервер безопасности станет неработоспособен и недоступен для связи с другими компонентами Secret Net Studio.

Установка сервера безопасности может выполняться в одном из следующих вариантов:

- установка с созданием нового леса и домена безопасности;
- установка с созданием нового домена безопасности в имеющемся лесу доменов безопасности;
- установка с включением сервера в состав имеющегося домена безопасности.

Создание леса и домена безопасности

При установке в системе первого сервера безопасности необходимо использовать вариант установки с созданием нового леса доменов безопасности и нового домена безопасности. Данный вариант также применяется для создания отдельного леса доменов безопасности.

Для установки сервера с созданием нового леса и домена безопасности:

1. Вставьте в привод установочный диск системы Secret Net Studio. Дождитесь появления окна программы автозапуска (см. стр.**48**) и запустите установку с помощью команды "Сервер безопасности".

   Примечание. Запуск установки можно выполнить вручную без использования программы автозапуска. Для этого запустите с установочного диска файл \Setup\Server\x64\ setup.ru-RU.exe.

   После запуска программы установки выполняется анализ системы на соответствие программным и аппаратным требованиям для установки компонента. При этом проверяется текущее состояние встроенного в ОС механизма управления учетными записями (UAC).

   Внимание! Если механизм UAC включен — на экране появится диалог запроса на его временное отключение. В этом случае нажмите кнопку "Да" для отключения механизма, перезагрузите компьютер и только после этого снова запустите процедуру установки сервера безопасности.

По окончании проверки системы на экран будет выведен диалог с перечнем устанавливаемых компонентов, позволяющий дополнительно выбрать для установки службу синхронизации.

Пояснение. Служба синхронизации устанавливается на сервере безопасности, чтобы, выполняя функцию шлюза, обеспечить взаимодействие этого сервера с родительским сервером безопасности. Установка данной службы выполняется отдельной программой установки, которая будет автоматически запущена после завершения установки сервера безопасности (см. стр.58).

2. Если требуется установить на данном сервере службу синхронизации, отметьте поле "Служба синхронизации". Нажмите кнопку "Установить".

   Программа установки сервера начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.

3. Для продолжения установки нажмите кнопку "Далее".

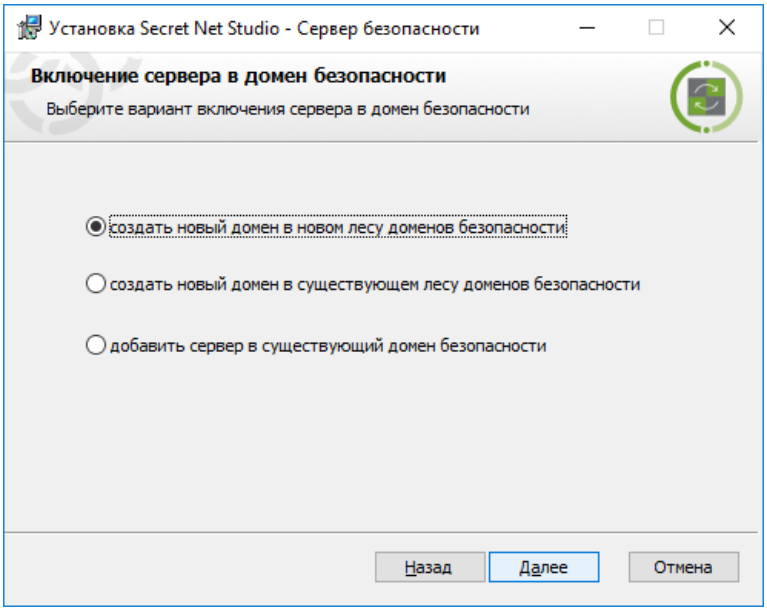
   На экране появится диалог принятия лицензионного соглашения.

4. Ознакомьтесь с содержанием лицензионного соглашения, отметьте пункт о его принятии и нажмите кнопку "Далее".

   Если на компьютере заняты порты для использования службами каталогов (любой порт из диапазона 50000–50003), на экране появится диалог для настройки использования портов.

5. В диалоге "Настройка портов служб каталогов" можно указать номера других портов вместо занятых или выполнить попытку переопределения занятых портов (с помощью кнопки "Зарезервировать") для использования сервером безопасности. Выполните нужные действия и нажмите кнопку "Далее".

   На экране появится диалог "Включение сервера в домен безопасности".



6. Установите отметку в поле "создать новый домен в новом лесу доменов безопасности" и нажмите кнопку "Далее".

   На экране появится диалог "Файл с настройками сервера аутентификации", предназначенный для создания файла с параметрами подключения сервера аутентификации в новом домене безопасности.

7. В диалоге укажите размещение и имя создаваемого файла и нажмите кнопку "Далее".

   Внимание! Файл с параметрами подключения содержит данные для доступа к серверу. Эти данные необходимы при добавлении других серверов безопасности в этот же домен безопасности. Для создаваемого файла необходимо обеспечить условия надежного хранения с защитой от компрометации содержащихся в нем данных.

   На экране появится диалог "Настройка домена безопасности".

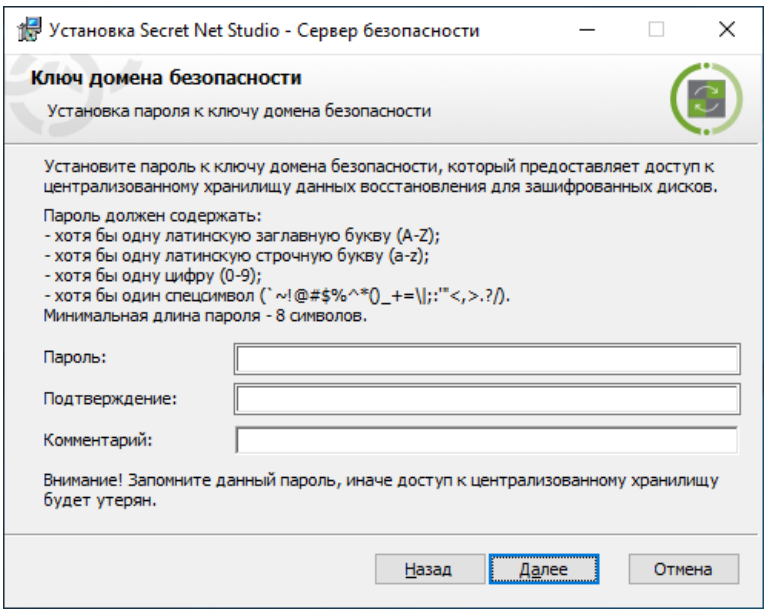
8. Выберите в раскрывающемся списке контейнер для формирования нового домена безопасности. В качестве контейнера можно выбрать организационное подразделение, в которое входит компьютер, или любое вышестоящее организационное подразделение (включая весь домен AD). После выбора контейнера при необходимости отредактируйте имя создаваемого домена безопасности.
9. Нажмите кнопку "Далее".

   На экране появится диалог "Группы администраторов безопасности".
10. Укажите группы пользователей, которым будут предоставлены права администрирования домена безопасности и леса доменов безопасности. Нажмите кнопку "Далее".

    Совет. В целях обеспечения безопасности информации разграничьте доступ администраторов, создав отдельную группу пользователей для администраторов домена безопасности. Использовать стандартную доменную группу администраторов (Domain Admins) не рекомендуется.

    На экране появится диалог "Настройка каталогов".
11. Оставьте заданные по умолчанию каталоги установки сервера безопасности и размещения служебных файлов или укажите другие пути назначения. Нажмите кнопку "Далее".

    На экране появится диалог "Ключ домена безопасности".

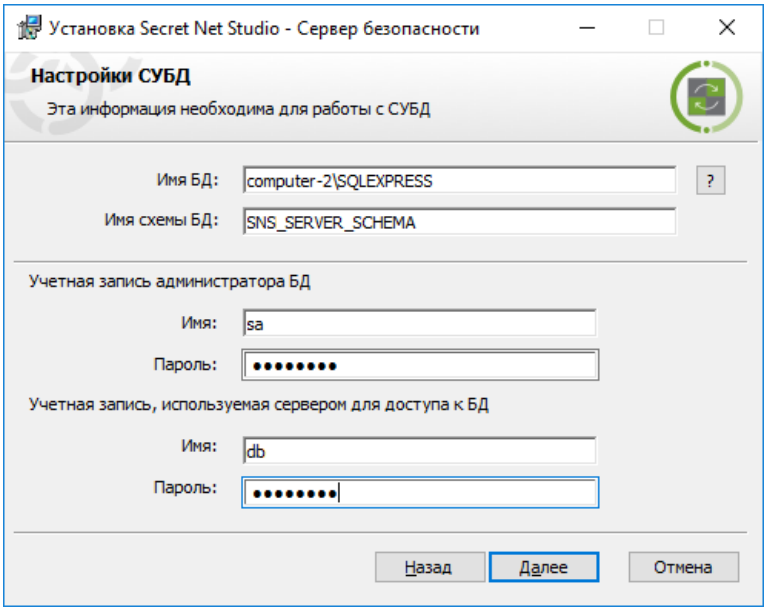


12. Установите пароль к ключу домена безопасности. Ключ и пароль предназначены для предоставления доступа к централизованному хранилищу данных восстановления для зашифрованных дисков. Пароль должен удовлетворять требованиям, указанным в диалоге.

    Внимание! Запомните пароль к ключу домена безопасности, иначе доступ к централизованному хранилищу данных восстановления будет утерян.

    Введите подтверждение пароля. При необходимости укажите комментарий к паролю. Нажмите кнопку "Далее".

    На экране появится диалог "Настройки СУБД". Пример содержимого диалога представлен на следующем рисунке.



13. Для настройки СУБД MS SQL выполните следующие действия:

- Укажите параметры соединения с тем экземпляром БД, который предназначен для работы с устанавливаемым сервером безопасности:
  - в поле "Имя БД" укажите расположение БД, используя следующий формат строки:

    <имя_или_IP-адрес_сервера_MS_SQL>\<имя_экземпляра_БД>,<порт>

    Примечание.
    - Если сервер СУБД установлен на компьютере с СБ и используется стандартный экземпляр MSSQLSERVER, то имя или IP-адрес сервера СУБД указывать не нужно.
    - Если для подключения используется порт по умолчанию, то порт можно не указывать.
  - в поле "Имя схемы БД" введите наименование схемы БД, которая будет создана;

    Примечание. Для каждого сервера безопасности создается отдельная схема БД.
  - в группу полей "Учетная запись администратора БД" введите учетные данные администратора БД на сервере СУБД;
  - в группу полей "Учетная запись, используемая сервером для доступа к БД" введите учетные данные, с которыми сервер безопасности будет выполнять подключение к БД (будет создана учетная запись для подключения).

    Примечание.
    - Сервер безопасности не поддерживает режим аутентификации Windows при работе с сервером СУБД. Поэтому для соединения с БД необходимо указывать учетные данные пользователя базы данных (не доменного пользователя).
    - Для учетных данных используйте латинские символы.
- Нажмите кнопку "Далее".

14. Если база данных уже существует (осталась от предыдущего установленного сервера), на экране появится диалог для выбора варианта дальнейших действий: использовать существующую базу данных или создать новую. В диалоге выберите нужный вариант и нажмите кнопку "Далее".

На экране появится диалог "Название организации".

15. Укажите названия организации и подразделения, которое будет обслуживать устанавливаемый сервер, и нажмите кнопку "Далее".

Примечание. Эти данные будут использоваться при генерации сертификата сервера безопасности. Названия организации и подразделения могут быть введены позднее или заменены другими при выполнении процедуры "Генерация и установка сертификата сервера безопасности".

На экране появится диалог, сообщающий о готовности к установке.

16. Нажмите кнопку "Установить".

Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса. При выполнении действий на экране могут появляться дополнительные окна, в которых выводятся служебные сведения об отдельных этапах. Окна закрываются автоматически после завершения этапов.

Примечание. Если пользователь, запустивший процесс установки сервера безопасности, не входит в группу администраторов домена безопасности, то на данном этапе установки будут запрошены учетные данные пользователя.

Если при выполнении действия **2** была выбрана установка службы синхронизации, будет запущена программа установки этой службы. Выполните ее установку так, как это описано на стр.**58**

После успешной установки и настройки на экране появится окно с перечнем операций программы установки. После завершения всех предусмотренных операций появится сообщение о необходимости перезагрузки компьютера.

17. Перезагрузите компьютер.

Внимание! Объект нового сервера безопасности может появиться в структуре оперативного управления с некоторой задержкой. В Центре управления, подключенном к другому серверу безопасности, загрузка обновленной структуры с новым сервером может произойти через несколько минут после установки ПО СБ (порядка 10–15 минут).

При первом запуске сервера безопасности выполняется синхронизация доменных пользователей, имеющихся в Active Directory, с базой данных СБ. В зависимости от количества учетных записей процесс синхронизации может занять от нескольких минут до одного часа. Рекомендуется дождаться завершения синхронизации и до этого времени не выполнять какие-либо действия с учетными записями, включая процедуру первого входа пользователя в систему на защищаемом компьютере. Если пользователь выполнит первый вход до завершения синхронизации, это может привести к сохранению неактуальных сведений о нем в базе данных сервера. В частности, возможна рассинхронизация сведений о пароле пользователя, после чего потребуется сменить пароль в программе управления пользователями Secret Net Studio.

Создание домена безопасности в имеющемся лесу

При наличии леса доменов безопасности (сформированного при установке первого сервера безопасности в этом лесу) можно создать новый домен безопасности и включить его в состав леса. Для этого необходимо выполнить установку нового сервера безопасности в варианте создания домена безопасности в имеющемся лесу.

Для установки сервера безопасности с созданием нового домена безопасности в имеющемся лесу:

1. Выполните действия **1–5** процедуры установки сервера с созданием нового леса и домена безопасности (см. стр.**52**).
2. В диалоге "Включение сервера в домен безопасности" установите отметку в поле "создать новый домен в существующем лесу доменов безопасности" и нажмите кнопку "Далее".

   На экране появится диалог "Файл с настройками сервера аутентификации", предназначенный для создания файла с параметрами подключения сервера аутентификации в новом домене безопасности.
3. В диалоге укажите размещение и имя создаваемого файла и нажмите кнопку "Далее".

Внимание! Файл с параметрами подключения содержит данные для доступа к серверу. Эти данные необходимы при добавлении других серверов безопасности в этот же домен безопасности. Для создаваемого файла необходимо обеспечить условия надежного хранения с защитой от компрометации содержащихся в нем данных.

На экране появится диалог "Подчинение сервера безопасности".

4. Выберите в раскрывающемся списке поля "Родительский сервер" имя компьютера, который будет являться родительским сервером безопасности. В поле "Настройки подключения" укажите шаблон сетевых параметров взаимодействия с родительским сервером.

Пояснение. Шаблон сетевых параметров взаимодействия определяет значения тайм-аутов в соответствии со скоростными параметрами сети. Значения тайм-аутов могут быть откорректированы позднее при настройке сервера безопасности в Центре управления.

5. Нажмите кнопку "Далее".

Примечание. Если пользователь, запустивший процесс установки сервера безопасности, не входит в группу администраторов леса безопасности, то на данном этапе установки будут запрошены учетные данные пользователя.

На экране появится диалог "Настройка домена безопасности".

6. Выберите в раскрывающемся списке контейнер для формирования нового домена безопасности. В качестве контейнера можно выбрать организационное подразделение, в которое входит компьютер с СБ, или любое вышестоящее организационное подразделение (включая весь домен AD). После выбора контейнера при необходимости отредактируйте имя создаваемого домена безопасности и нажмите кнопку "Далее".

   На экране появится диалог "Группы администраторов безопасности".

7. В диалоге "Группы администраторов безопасности" укажите группу пользователей, которым будут предоставлены права администрирования домена безопасности. Нажмите кнопку "Далее".

   На экране появится диалог "Настройка каталогов". Далее выполните завершающие действия процедуры установки сервера с созданием нового леса и домена безопасности (см. стр.**52**), начиная с действия **11**.

Добавление сервера в имеющийся домен безопасности

При наличии домена безопасности (сформированного при установке первого сервера безопасности в этом домене) можно включить в его состав дополнительный сервер безопасности. Для этого необходимо выполнить установку нового сервера безопасности в варианте включения в состав имеющегося домена безопасности.

Для установки сервера безопасности с включением сервера в состав имеющегося домена безопасности:

1. Выполните действия **1–5** процедуры установки сервера с созданием нового леса и домена безопасности (см. стр.**52**).
2. В диалоге "Включение сервера в домен безопасности" установите отметку в поле "добавить сервер в существующий домен безопасности" и нажмите кнопку "Далее".

   На экране появится диалог "Файл с настройками сервера аутентификации", предназначенный для выбора файла с параметрами подключения сервера аутентификации в целевом домене безопасности.
3. В диалоге укажите размещение и имя файла, созданного при установке первого сервера в этом домене безопасности, и нажмите кнопку "Далее".

Внимание! Для файла с параметрами подключения необходимо обеспечить безопасную передачу на компьютер, чтобы не допустить компрометации содержимого файла.

На экране появится диалог "Подчинение сервера безопасности".

4. Выберите в раскрывающемся списке поля "Родительский сервер" имя компьютера, который будет являться родительским сервером безопасности. В поле "Настройки подключения" укажите шаблон сетевых параметров взаимодействия с родительским сервером.

   Пояснение. Шаблон сетевых параметров взаимодействия определяет значения тайм-аутов в соответствии со скоростными параметрами сети. Значения тайм-аутов могут быть откорректированы позднее при настройке сервера безопасности в Центре управления.

5. Нажмите кнопку "Далее".

   На экране появится окно с информацией о домене безопасности родительского сервера.

6. Нажмите кнопку "Далее".

   Примечание. Если пользователь, запустивший процесс установки сервера безопасности, не входит в группу администраторов леса и домена безопасности, то на данном этапе установки будут запрошены учетные данные пользователя.

   На экране появится диалог "Настройка каталогов". Далее выполните завершающие действия процедуры установки сервера с созданием нового леса и домена безопасности (см. стр.**52**), начиная с действия **11**.

Установка ПО шлюза

Программное обеспечение шлюза — служба синхронизации — входит в состав сервера безопасности и может устанавливаться в процессе его установки либо отдельно. Программа установки службы синхронизации запускается программой установки сервера безопасности после выбора этого компонента при выполнении следующих операций:

- установка нового сервера безопасности;
- обновление существующего сервера безопасности до новой версии;
- повторный запуск программы установки для существующего сервера безопасности той же версии — используйте этот вариант для установки ПО шлюза на уже имеющийся и функционирующий сервер безопасности.

Внимание! При выборе к установке службы синхронизации для успешного ее завершения необходимо соблюдать следующие условия:

- на родительском сервере безопасности в Центре управления должен быть зарегистрирован соответствующий шлюз;
- дочерний сервер безопасности должен иметь в наличии специальный файл (pav) с параметрами данного шлюза;
- на момент установки компьютер с дочерним сервером безопасности должен иметь возможность устанавливать сетевое соединение с компьютером, на котором функционирует родительский сервер безопасности, по полному DNS-имени этого компьютера.

Для установки службы синхронизации:

1. После выполнения подготовительных действий и появления на экране диалога приветствия программы установки службы синхронизации нажмите кнопку "Далее".

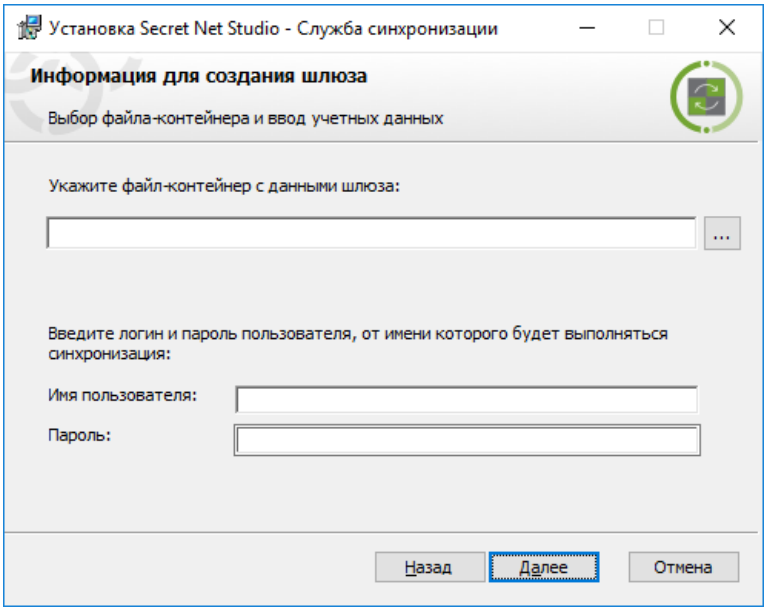
   На экране появится диалог принятия лицензионного соглашения.

2. Ознакомьтесь с содержанием лицензионного соглашения, отметьте пункт о его принятии и нажмите кнопку "Далее".

   На экране появится диалог "Конечная папка".

3. Оставьте заданную по умолчанию папку установки ПО или укажите другую папку назначения и нажмите кнопку "Далее".

   На экране появится следующий диалог.



4. Введите в полях диалога информацию, необходимую для создания шлюза.
   - Укажите путь к специальному файлу с параметрами шлюза. Для этого нажмите кнопку справа от поля и выберите нужный файл в появившемся стандартном диалоге.
   - Введите имя пользователя и его пароль, которые были заданы при регистрации данного шлюза в корневом (родительском) лесу безопасности.
   - Нажмите кнопку "Далее".

   Если все сведения указаны верно, на экране появится диалог с информацией о создаваемом шлюзе.
5. Нажмите кнопку "Далее".

   При успешной проверке доступности нужного сервера безопасности на экране появится диалог, сообщающий о готовности к установке.
6. Нажмите кнопку "Установить".

   Начнется процесс установки службы синхронизации, ход которого отображается в информационном окне в виде полосы прогресса. При его успешном завершении на экране появится диалог с сообщением об этом.
7. Нажмите кнопку "Готово".

   На завершающем этапе управление будет передано программе установки сервера безопасности. Выполните все предлагаемые ею действия, включая перезагрузку компьютера.

Установка Центра управления

Для установки Центра управления:

1. Вставьте в привод установочный диск системы Secret Net Studio. Дождитесь появления окна программы автозапуска (см. стр.**48**) и нажмите в нем кнопку "Центр управления".

   Совет. Для запуска установки без использования программы автозапуска:
   - на компьютере с 64-разрядной версией Windows — запустите с установочного диска файл \Setup\Console\x64\setup.ru-RU.exe;
   - на компьютере с 32-разрядной версией Windows — запустите с установочного диска файл \Setup\Console\Win32\setup.ru-RU.exe.

   Программа установки выполнит подготовительные действия, по окончании которых на экране появится диалог приветствия.
2. Для продолжения установки нажмите кнопку "Далее".

   На экране появится диалог принятия лицензионного соглашения.

3. Ознакомьтесь с содержанием лицензионного соглашения, отметьте соответствующий принятию соглашения пункт и нажмите кнопку "Далее".

   На экране появится диалог "Конечная папка".

4. Оставьте заданную по умолчанию папку установки ПО или укажите другую папку назначения и нажмите кнопку "Далее".

   На экране появится диалог, сообщающий о готовности к установке.

5. Нажмите кнопку "Установить".

   Начнется процесс установки, ход которого отображается в информационном окне в виде полосы прогресса. После успешной установки на экране появится диалог "Установка завершена".

6. Нажмите кнопку "Готово", а затем нажмите кнопку "Закрыть" в еще одном появившемся на экране диалоге.

Установка клиента

Локальная установка компонента "Secret Net Studio" выполняется при невозможности или нецелесообразности применения централизованной установки клиента (см. стр. **64**). В частности, для установки в автономном режиме функционирования.

Установка клиента в интерактивном режиме

Для установки клиента:

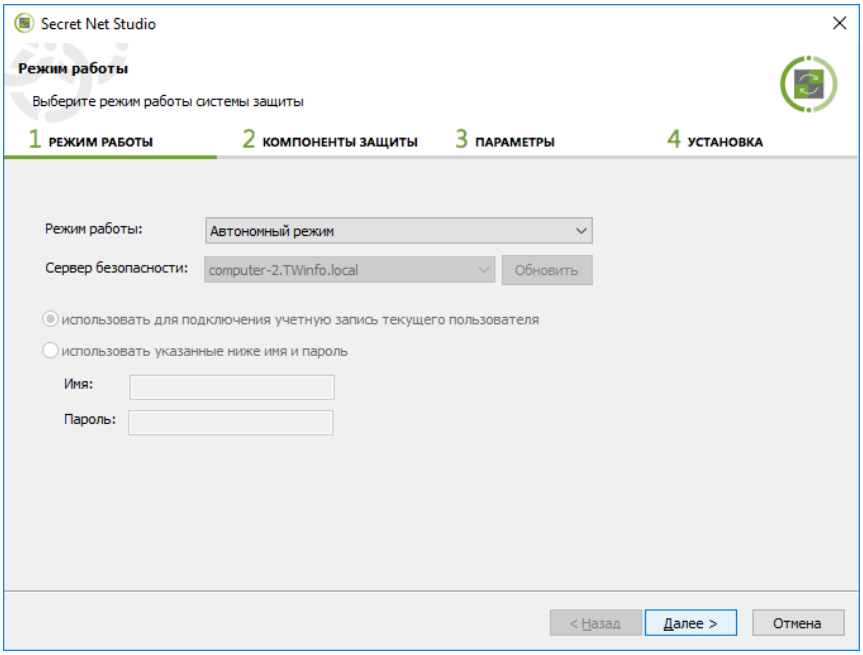
1. Вставьте в привод установочный диск системы Secret Net Studio. Дождитесь появления окна программы автозапуска (см. стр. **48**) и запустите установку с помощью команды "Защитные компоненты".

   Примечание. Запуск установки можно выполнить вручную без использования программы автозапуска. Для этого в зависимости от операционной системы компьютера выполните следующее действие:
   - при установке на компьютер с 64-разрядной версией Windows — запустите с установочного диска файл \Setup\Client\x64\SnSetup.ru-RU.exe;
   - при установке на компьютер с 32-разрядной версией Windows — запустите с установочного диска файл \Setup\Client\Win32\SnSetup.ru-RU.exe.

   На экране появится диалог принятия лицензионного соглашения.

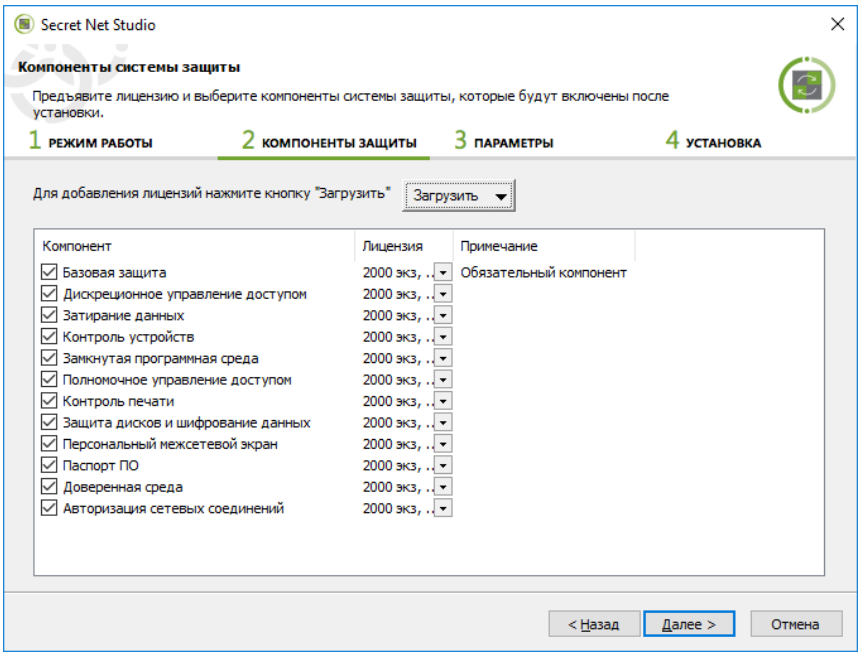
2. Ознакомьтесь с содержанием лицензионного соглашения и нажмите кнопку "Принимаю".

   На экране появится диалог для выбора режима работы компонента.



3. В поле "Режим работы" укажите нужный режим функционирования клиента — автономный ("Автономный режим") или сетевой ("Под управлением сервера безопасности"). Для сетевого режима функционирования настройте параметры подчинения серверу безопасности:
   - Выберите имя компьютера сервера безопасности, которому будет подчинен данный компьютер (если в раскрывающемся списке отсутствует имя нужного сервера, нажмите кнопку "Обновить").
   - Для подчинения компьютера необходимы права на администрирование домена безопасности, к которому относится сервер. Если пользователь, выполняющий установку, обладает такими правами, оставьте отмеченным поле "использовать для подключения учетную запись текущего пользователя". В противном случае установите отметку в поле "использовать указанные ниже имя и пароль" и введите учетные данные пользователя из группы администраторов домена безопасности.
4. Нажмите кнопку "Далее >".

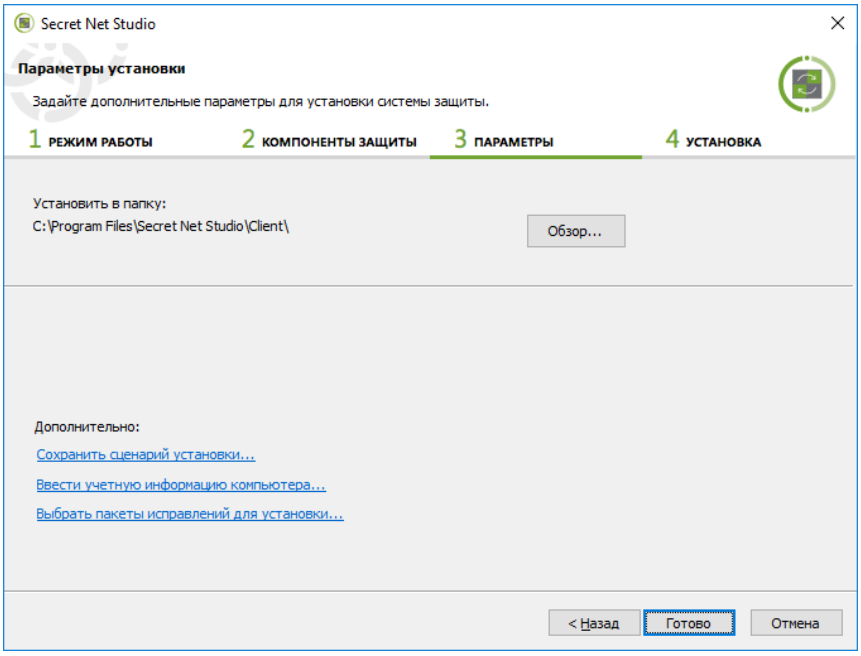
   На экране появится диалог для выбора лицензий и формирования списка устанавливаемых защитных подсистем.



5. Нажмите кнопку "Загрузить" и выберите из раскрывающегося списка метод получения лицензий:
   - чтобы загрузить лицензии с сервера безопасности, который был выбран для подчинения — укажите "С сервера безопасности";
   - чтобы загрузить лицензии из файла (в частности, при установке клиента в автономном режиме функционирования) — укажите "Из файла", а затем выберите нужный файл в появившемся диалоге.

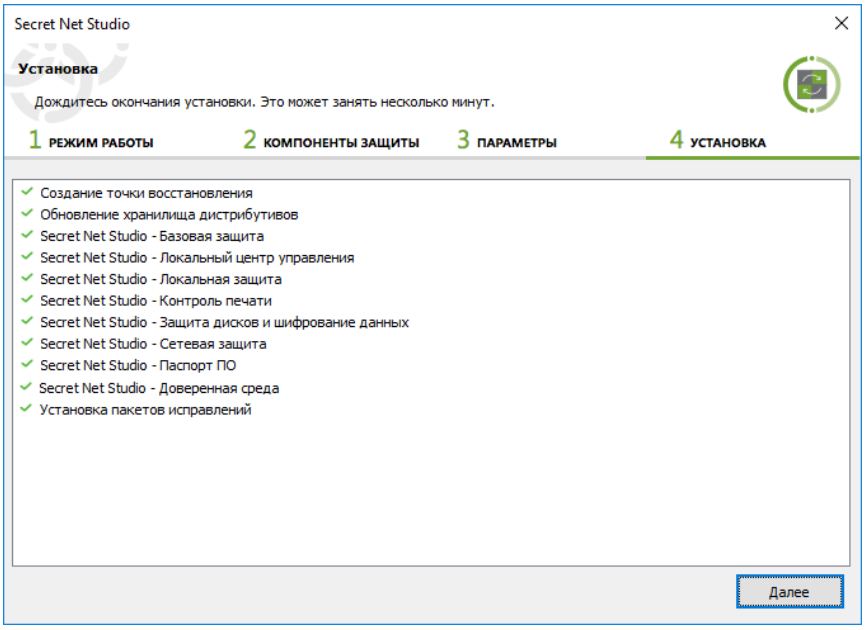
   После загрузки данных в диалоге появятся сведения о лицензиях.
6. Отметьте в списке устанавливаемые подсистемы, для которых имеются свободные лицензии (установку компонента "Базовая защита" отключить нельзя). При наличии нескольких групп лицензий для компонента можно выбрать нужную группу в раскрывающемся списке.
7. Нажмите кнопку "Далее >".

   На экране появится диалог для выбора папки установки клиента и настройки параметров подключений.



8. В поле "Установить в папку" оставьте заданную по умолчанию папку установки клиента или укажите другую папку назначения.
9. При необходимости используйте ссылки в разделе "Дополнительно" для выполнения следующих действий:
   - чтобы сохранить заданные параметры установки в файле — выберите ссылку "Сохранить сценарий установки". Файл сценария установки можно использовать для автоматизации процесса установки клиентского ПО на других компьютерах;
   - чтобы ввести сведения о компьютере для учета — выберите ссылку "Ввести учетную информацию компьютера";
   - чтобы просмотреть и выбрать пакеты исправлений, которые будут применены при установке, — выберите ссылку "Выбрать пакеты исправлений для установки".
10. По окончании настройки параметров нажмите кнопку "Готово".

    Начнется процесс установки защитных подсистем в соответствии с заданными параметрами.



11. После завершения всех операций установки нажмите кнопку "Далее".

    На экране появится завершающий диалог со сведениями о выполненных операциях.

12. Проверьте состав подключенных к компьютеру устройств. Если подключены устройства, которые в дальнейшем должны быть запрещены к использованию, — отключите их.

> **Внимание!** При первой загрузке компьютера после установки клиентского ПО текущая аппаратная конфигурация автоматически принимается в качестве эталонной. Поэтому до перезагрузки необходимо отключить те устройства, которые должны быть запрещены к использованию на данном компьютере.

> **Совет.** При необходимости используйте ссылки в разделе "Информация" для выполнения следующих действий:
> - чтобы посмотреть записи журнала трассировки — выберите ссылку "отчет об установке";
> - чтобы собрать все необходимые для диагностики Secret Net Studio – C файлы и данные, в случае возникновения проблем при установке — выберите ссылку "диагностическую информацию".

13. Перезагрузите компьютер и дождитесь загрузки системы.

Глава 7
Централизованное развертывание системы

Установка под управлением сервера безопасности

Централизованное развертывание ПО клиента под управлением сервера безопасности инициируется средствами Центра управления.

При развертывании автоматически выполняются заданные действия по установке или удалению на компьютерах клиента Secret Net Studio, его компонентов, обновлений или пакетов обновлений. Запуск установки, обновления, исправления, удаления ПО или пакетов обновлений на компьютерах осуществляется под управлением сервера безопасности от имени специальной службы.

На клиентских компьютерах установка ПО выполняется автоматически в фоновом режиме. Пользователь оповещается о начале и завершении процесса установки. В ходе этого процесса, в зависимости от настройки параметров задания развертывания, пользователю будет предложено самостоятельно перезагрузить компьютер или перезагрузка произойдет автоматически.

Внимание! Для централизованного развертывания ПО компьютеры должны удовлетворять требованиям к аппаратному и программному обеспечению для установки клиента (см. стр.45). В частности, необходимо разрешить использование портов для доступа к общим ресурсам: 137, 138, 139, 445. Данные порты по умолчанию закрыты брандмауэром при отсутствии на компьютере сетевых папок общего доступа.

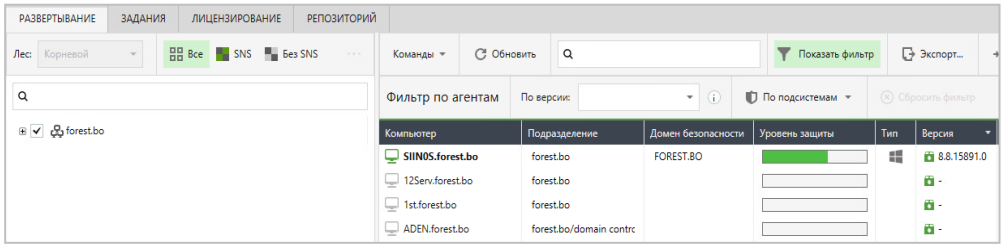
Перечень предусмотренных операций представлен в таблице.

Операция	Описание
Установка ПО	Выполняется установка программного обеспечения клиента. Для установки ПО на компьютерах средствами Центра управления необходимо выполнить следующие действия: **1.** Зарегистрировать лицензии на защитные подсистемы (см. стр.**66**). **2.** Сформировать список устанавливаемого ПО, добавив в репозиторий комплект установочных файлов (см. стр.**69**). **3.** Добавить задание для установки (см. стр.**70**): • выбрать компьютеры, для которых нужно сформировать задание; • настроить параметры задания: версия устанавливаемого ПО, папка для установки ПО, время ожидания перезагрузки компьютера после установки, параметры командной строки, с которыми будет запущена программа установки, лицензии на использование компонентов, пакеты обновлений, учетные данные доменного пользователя, входящего в группу локальных администраторов на выбранных компьютерах, а также обладающего привилегией интерактивного входа в систему. **4.** Дождаться выполнения задания и проконтролировать процесс установки ПО (см. стр.**72**)
Обновление ПО	Выполняется обновление установленной ранее версии программного обеспечения клиента на новую. Для обновления ПО на компьютерах средствами Центра управления необходимо выполнить следующие действия: **1.** Сформировать список устанавливаемого ПО, добавив в репозиторий последнюю версию комплекта установочных файлов (см. стр.**69**). **2.** Добавить задание для обновления (см. стр.**70**): • выбрать компьютеры, для которых нужно сформировать задание; • настроить параметры задания: время ожидания перезагрузки компьютера перед установкой, версия обновления ПО, пакеты обновлений. **3.** Дождаться выполнения задания и проконтролировать процесс обновления ПО (см. стр.**72**)

Операция	Описание
Исправление ПО	Выполняется исправление установленного ранее программного обеспечения клиента. Для исправления ПО на компьютерах средствами Центра управления необходимо выполнить следующие действия: **1.** Выбрать компьютеры, для которых нужно сформировать задание. **2.** Добавить задание для исправления (см. стр.**70**): • настроить параметр задания: время ожидания перезагрузки компьютера перед исправлением. **3.** Дождаться выполнения задания и проконтролировать процесс исправления ПО (см. стр.**72**)
Удаление ПО	Выполняется удаление установленного программного обеспечения клиента. Для удаления ПО на компьютерах средствами Центра управления необходимо выполнить следующие действия: **1.** Выбрать компьютеры, для которых нужно сформировать задание. **2.** Добавить задание для удаления (см. стр.**70**): • настроить параметр задания: время ожидания перезагрузки компьютера после удаления. **3.** Дождаться выполнения задания и проконтролировать процесс удаления ПО (см. стр.**72**)
Установка пакетов исправлений	Выполняется установка пакетов обновлений. Для установки пакетов обновлений на компьютерах средствами Центра управления необходимо выполнить следующие действия: **1.** Сформировать список устанавливаемого ПО, добавив в репозиторий пакеты обновлений (см. стр.**69**). **2.** Добавить задание для установки пакетов обновлений (см. стр.**70**): • выбрать компьютеры, для которых нужно сформировать задание; • настроить параметры задания: время ожидания перезагрузки компьютера перед установкой, выбрать необходимые пакеты обновлений для установки. **3.** Дождаться выполнения задания и проконтролировать процесс установки пакетов обновлений (см. стр.**72**)
Удаление всех пакетов исправлений	Выполняется удаление всех установленных ранее пакетов обновлений. Для удаления всех пакетов обновлений на компьютерах средствами Центра управления необходимо выполнить следующие действия: **1.** Выбрать компьютеры, для которых нужно сформировать задание. **2.** Добавить задание для удаления всех пакетов обновлений (см. стр.**70**): • настроить параметр задания: время ожидания перезагрузки компьютера перед удалением. **3.** Дождаться выполнения задания и проконтролировать процесс удаления всех пакетов обновлений (см. стр.**72**)

Панель средств настройки и контроля

Настройка и контроль централизованного развертывания ПО осуществляются в панели "Развертывание". Панель имеет вид, подобный представленному на рисунке ниже.



Для работы со средствами настройки и контроля развертывания ПО в панели предусмотрены следующие вкладки:

- "Развертывание" — предназначена для отображения структуры управления (слева) и вывода списка компьютеров со сведениями о наличии ПО и статусе (справа);
- "Задания" — предназначена для отображения заданий развертывания (слева) и компьютеров, связанных с заданиями (справа);
- "Лицензирование" — предназначена для просмотра сведений о зарегистрированных лицензиях на сервере безопасности и управления лицензиями;
- "Репозиторий" — предназначена для формирования списка централизованно устанавливаемого ПО.

Переключение между вкладками осуществляется с помощью соответствующих кнопок в верхней части панели.

Управление лицензиями на использование механизмов защиты

В системе Secret Net Studio действуют лицензионные ограничения на использование подсистем, реализующих применение механизмов защиты. Лицензии поставляются в виде файлов, содержащих данные для регистрации в системе Secret Net Studio.

Внимание! Если срок действия лицензии истек, то ее невозможно использовать для установки клиентского ПО. Если лицензия не активирована, то возможна интерактивная установка клиентского ПО.

Если лицензия хотя бы на одну работающую подсистему не активирована или ее срок действия истек, то клиентское ПО переходит в ограниченный режим работы, при котором невозможно редактировать настройки системы защиты, а также запускать большую часть защитных утилит.

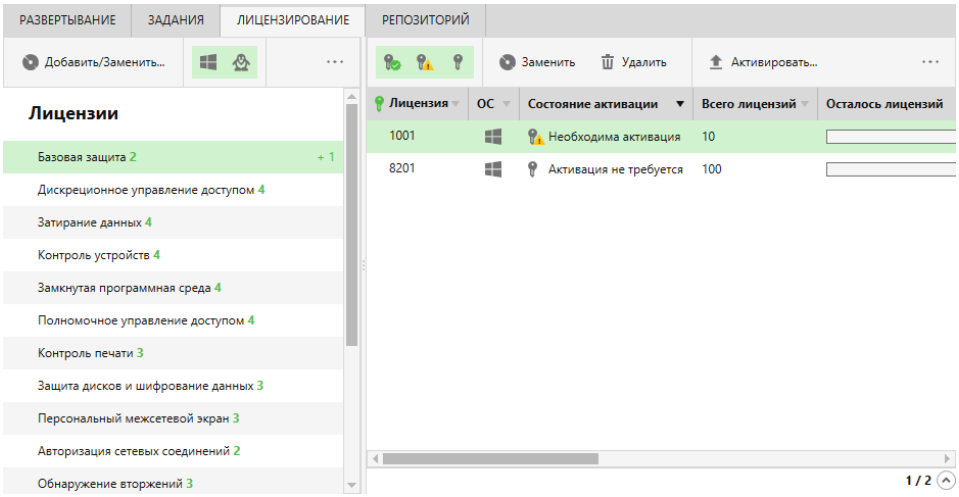
При формировании заданий развертывания ПО (см. стр.**70**) необходимо указать соответствующие лицензии. Лицензии можно выбрать из списка зарегистрированных на сервере безопасности или добавить отдельно для задания развертывания.

Для управления зарегистрированными лицензиями используется вкладка "Лицензирование" в панели "Развертывание". Вкладка содержит сведения о лицензиях, зарегистрированных в домене безопасности сервера подключения (сервер безопасности, с которым установлено соединение программы):

- назначение лицензий (для каких подсистем применяются);
- тип операционной системы, для которой предназначены лицензии (Windows/Linux);
- состояние активации лицензий;
- общее количество и текущее количество незадействованных (оставшихся) лицензий;
- время окончания действия лицензированных возможностей;
- типы лицензий;
- сведения о компании — получателе лицензии.

Для регистрации лицензий:

1. В панели "Развертывание" перейдите на вкладку "Лицензирование".



2. Нажмите кнопку "Добавить/Заменить", которая расположена над списком лицензируемых подсистем в разделе "Лицензии".

   На экране появится диалог для выбора файла.

3. Выберите нужный файл с лицензиями и нажмите кнопку "Применить".

4. Если лицензии не активированы, нажмите кнопку "Вперед". Выберите требуемый вариант активации лицензий и нажмите кнопку "Применить".

5. При выборе активации через личный кабинет загрузите файл запроса на страницу активации в личном кабинете, дождитесь активации лицензии и скачайте файл с активированными лицензиями.

   Добавьте файл с активированными лицензиями на сервер и подтвердите операцию замены.

Для замены зарегистрированных лицензий:

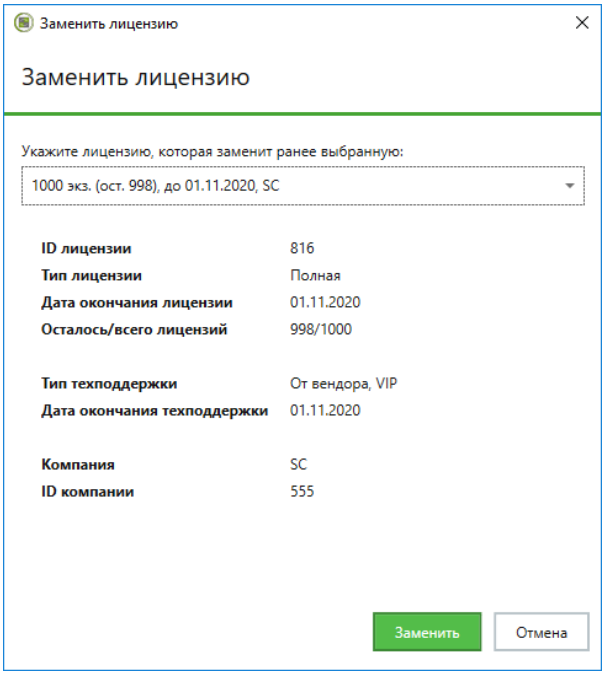
1. В панели "Развертывание" перейдите на вкладку "Лицензирование".

2. В списке "Лицензии" (слева) выберите подсистему, для которой нужно заменить используемые лицензии.

3. В списке доступных лицензий на использование подсистемы (справа) выберите лицензии для замены.

4. Нажмите кнопку "Заменить", которая расположена над списком лицензий.

   На экране появится диалог для выбора лицензии.



5. Выберите лицензию в раскрывающемся списке и нажмите кнопку "Заменить".

Для удаления зарегистрированных лицензий:

1. В панели "Развертывание" перейдите на вкладку "Лицензирование".
2. В списке "Лицензии" (слева) выберите подсистему, для которой нужно удалить используемые лицензии.
3. В списке доступных лицензий на использование подсистемы (справа) выберите лицензии для удаления.

Примечание. Удаление лицензии невозможно, если она используется хотя бы на одном защищаемом компьютере.

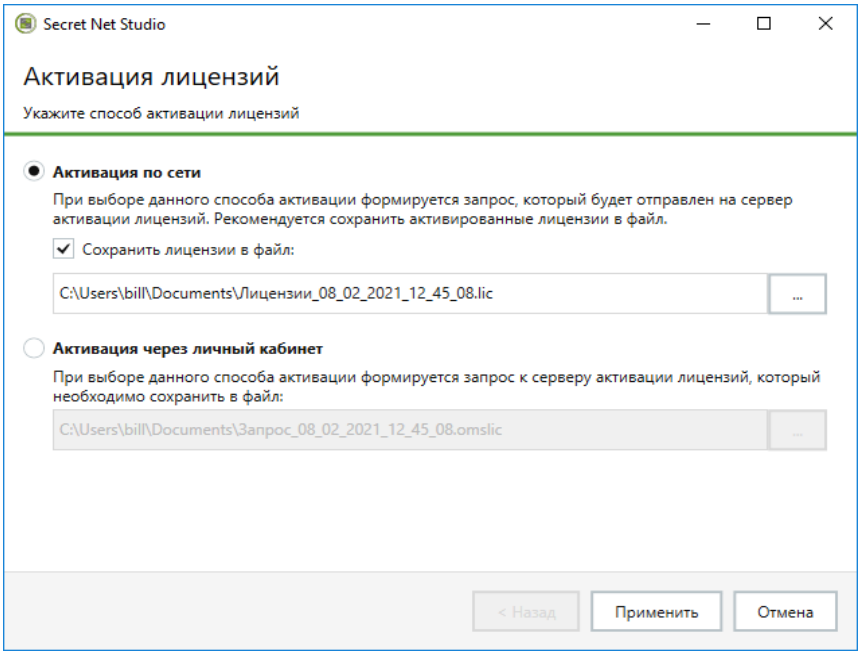
4. Нажмите кнопку "Удалить", которая расположена над списком лицензий.

   На экране появится запрос на продолжение операции.
5. Нажмите кнопку "Да" в диалоге запроса.

Для активации зарегистрированных лицензий:

1. В панели "Развертывание" перейдите на вкладку "Лицензирование".
2. В списке "Лицензии" (слева) выберите подсистему, для которой нужно активировать лицензии.
3. В списке доступных лицензий (справа) выберите лицензии для активации.
4. Нажмите кнопку "Активировать", которая расположена над списком лицензий.

   На экране появится диалог для активации лицензии.



5. Выберите вариант активации лицензии и нажмите кнопку "Применить".
6. При выборе активации через личный кабинет загрузите файл запроса на страницу активации в личном кабинете, дождитесь активации лицензии и скачайте файл с активированными лицензиями.

   Добавьте файл с активированными лицензиями на сервер и подтвердите операцию замены.

Для деактивации зарегистрированных лицензий:

1. В панели "Развертывание" перейдите на вкладку "Лицензирование".
2. В списке "Лицензии" (слева) выберите подсистему, для которой нужно деактивировать лицензии.
3. В списке доступных лицензий (справа) выберите лицензии для деактивации.

Примечание. Деактивация лицензии невозможна, если она используется хотя бы на одном защищаемом компьютере.

4. Нажмите кнопку "Деактивировать", которая расположена над списком лицензий.

   На экране появится диалог для деактивации лицензии.

5. Выберите вариант деактивации лицензии и нажмите кнопку "Применить".

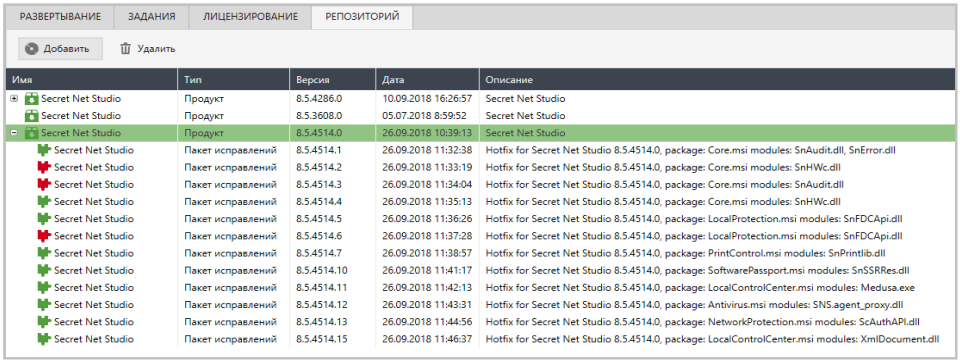
Формирование списка централизованно устанавливаемого ПО

По умолчанию список централизованно устанавливаемого ПО не заполнен. Для настройки развертывания необходимо добавить в список комплект (комплекты) установочных файлов. Комплект может быть создан на основе установочного диска системы Secret Net Studio или пакета обновлений ("патч").

Внимание! Комплекты установочных файлов помещаются в каталог Repository. Этот каталог создается при установке сервера безопасности в каталоге установки сервера и ему назначаются нужные права общего доступа. Не меняйте права доступа к данному каталогу, иначе централизованная установка ПО станет невозможна.

Для добавления комплекта установочных файлов:

1. В панели "Развертывание" перейдите на вкладку "Репозиторий".



Имя	Тип	Версия	Дата	Описание
Secret Net Studio	Продукт	8.5.4286.0	10.09.2018 16:26:57	Secret Net Studio
Secret Net Studio	Продукт	8.5.3608.0	05.07.2018 8:59:52	Secret Net Studio
Secret Net Studio	Продукт	8.5.4514.0	26.09.2018 10:39:13	Secret Net Studio
Secret Net Studio	Пакет исправлений	8.5.4514.1	26.09.2018 11:32:38	Hotfix for Secret Net Studio 8.5.4514.0, package: Core.msi modules: SnAudit.dll, SnError.dll
Secret Net Studio	Пакет исправлений	8.5.4514.2	26.09.2018 11:33:19	Hotfix for Secret Net Studio 8.5.4514.0, package: Core.msi modules: SnHWc.dll
Secret Net Studio	Пакет исправлений	8.5.4514.3	26.09.2018 11:34:04	Hotfix for Secret Net Studio 8.5.4514.0, package: Core.msi modules: SnAudit.dll
Secret Net Studio	Пакет исправлений	8.5.4514.4	26.09.2018 11:35:13	Hotfix for Secret Net Studio 8.5.4514.0, package: Core.msi modules: SnHWc.dll
Secret Net Studio	Пакет исправлений	8.5.4514.5	26.09.2018 11:36:26	Hotfix for Secret Net Studio 8.5.4514.0, package: LocalProtection.msi modules: SnFDCApi.dll
Secret Net Studio	Пакет исправлений	8.5.4514.6	26.09.2018 11:37:28	Hotfix for Secret Net Studio 8.5.4514.0, package: LocalProtection.msi modules: SnFDCApi.dll
Secret Net Studio	Пакет исправлений	8.5.4514.7	26.09.2018 11:38:57	Hotfix for Secret Net Studio 8.5.4514.0, package: PrintControl.msi modules: SnPrintlib.dll
Secret Net Studio	Пакет исправлений	8.5.4514.10	26.09.2018 11:41:17	Hotfix for Secret Net Studio 8.5.4514.0, package: SoftwarePassport.msi modules: SnSSRRes.dll
Secret Net Studio	Пакет исправлений	8.5.4514.11	26.09.2018 11:42:13	Hotfix for Secret Net Studio 8.5.4514.0, package: LocalControlCenter.msi modules: Medusa.exe
Secret Net Studio	Пакет исправлений	8.5.4514.12	26.09.2018 11:43:31	Hotfix for Secret Net Studio 8.5.4514.0, package: Antivirus.msi modules: SNS.agent_proxy.dll
Secret Net Studio	Пакет исправлений	8.5.4514.13	26.09.2018 11:44:56	Hotfix for Secret Net Studio 8.5.4514.0, package: NetworkProtection.msi modules: ScAuthAPI.dll
Secret Net Studio	Пакет исправлений	8.5.4514.15	26.09.2018 11:46:37	Hotfix for Secret Net Studio 8.5.4514.0, package: LocalControlCenter.msi modules: XmlDocument.dll

Пояснение. Пиктограммы пакетов исправлений, отмеченные красным цветом, являются обязательными обновлениями.

2. Нажмите кнопку "Добавить", которая расположена под вкладкой "Развертывание".

   На экране появится диалог для добавления комплекта установочных файлов.

3. В появившемся диалоге нажмите кнопку "Добавить".

   На экране появится диалог для выбора папки, содержащей комплект установочных файлов.

4. В поле "Папка" укажите каталог с файлами для создания установочного комплекта и нажмите кнопку "Выбор папки". Например, если комплект нужно создать на основе установочного диска системы Secret Net Studio и пакета обновлений — укажите корневой каталог установочного диска. Если комплект нужно создать только на основе пакета обновлений — укажите корневой каталог пакета обновлений, который находится на установочном диске в каталоге \Tools\SecurityCode\Patches. Пакет обновлений добавится в список централизованно устанавливаемого ПО только при наличии добавленного ранее в репозитории установочного диска системы Secret Net Studio.

   Внимание! Версии установочного комплекта системы Secret Net Studio и пакета обновлений должны быть одинаковы.

   В диалоге для добавления комплекта установочных файлов появится новый элемент списка, содержащий сведения о загруженном комплекте.

5. Нажмите кнопку "Применить".

На экране появится диалог процесса добавления файлов. Дождитесь окончания процедуры создания комплекта (процесс отправки файлов на сервер безопасности может занять продолжительное время).

6. Нажмите кнопку "Закрыть".

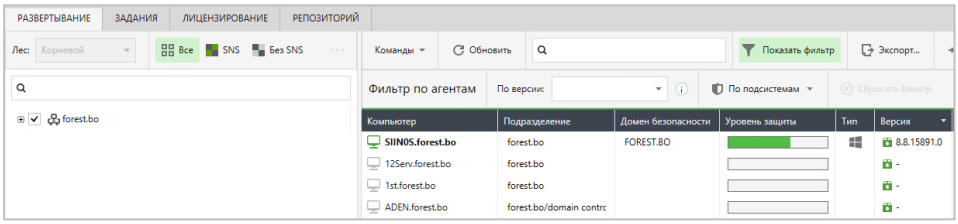
   По окончании процесса в списке появится новый элемент, содержащий сведения о загруженном комплекте.

Формирование заданий развертывания

После формирования списка централизованно устанавливаемого ПО необходимо добавить задания развертывания. Задания определяют списки компьютеров, на которых в автоматическом режиме будут выполняться нужные действия.

Для добавления задания развертывания:

1. В панели "Развертывание" перейдите на вкладку "Развертывание".



2. При наличии нескольких лесов настройте отображение структуры управления с помощью раскрывающегося списка "Лес".
3. Выберите компьютеры, для которых нужно сформировать задание. При необходимости используйте возможности фильтрации, сортировки и вывода сведений о компьютерах.

   Список компьютеров можно фильтровать по наличию или отсутствию установленного ПО клиента (кнопки "SNS", "Без SNS"), по принадлежности контейнерам Active Directory (отображаются компьютеры тех контейнеров, которые отмечены в структуре управления слева), а также по наличию в названии заданной строки символов (поля для поиска расположены над списком контейнеров AD и над таблицей со списком компьютеров).

   Сортировка списка компьютеров выполняется стандартными методами с помощью заголовков колонок.

   Компьютеры, подчиненные серверу безопасности, отмечены в списке зеленой пиктограммой и полужирным шрифтом.

   Для просмотра подробных сведений о компьютере выберите строку с ним двойным щелчком мыши или воспользуйтесь кнопкой с изображением стрелки в правой части строки под списком компьютеров.

   В таблице можно изменять состав отображаемых колонок и порядок их следования. Чтобы настроить колонки, вызовите контекстное меню в строке заголовков, выберите команду "Настройка колонок" и в появившемся диалоге сформируйте список отображаемых колонок.

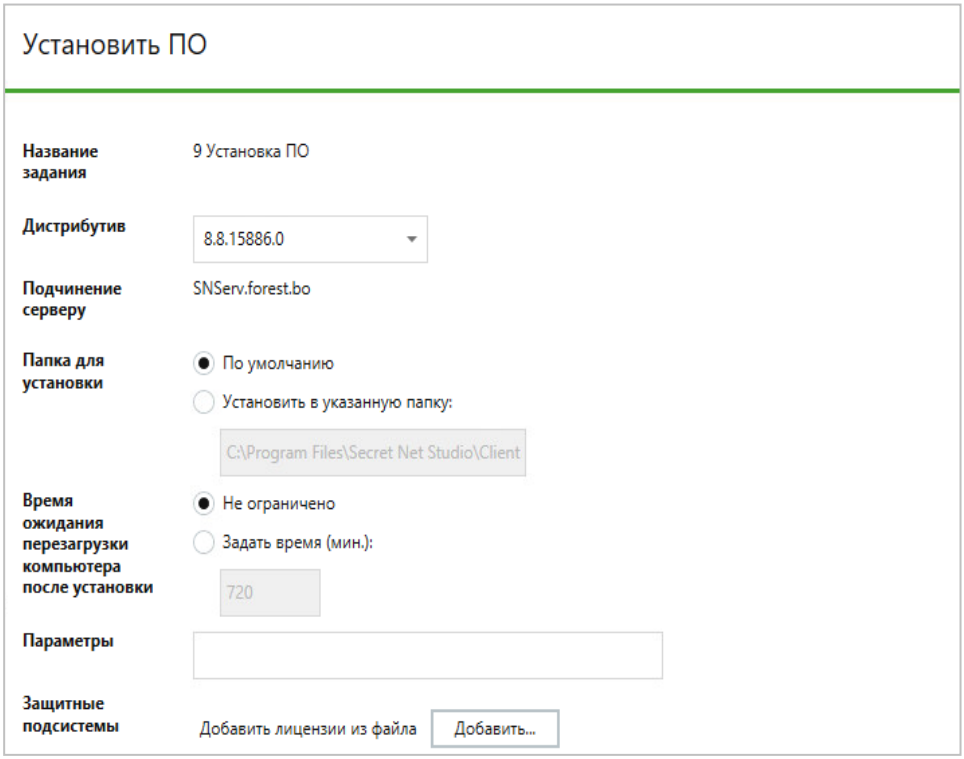
> **Примечание.** Если на компьютере установлено ПО клиента, полные сведения о его версии и установленных защитных подсистемах выводятся при подключении Центра управления к серверу безопасности, которому непосредственно подчинен данный компьютер. В случае подключения к другому серверу в том же домене безопасности для этого компьютера отображается только признак наличия ПО клиента. Сведения о составе установленных защитных подсистем в этом случае недоступны.

4. Вызовите контекстное меню одного из выбранных компьютеров и выберите нужную команду. Перечень предусмотренных команд представлен в таблице.

Команда	Описание
Установить ПО	Выполняется установка программного обеспечения клиента (подробное описание настройки параметров задания см. ниже)

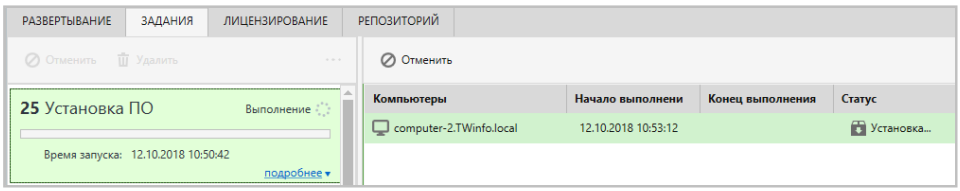
Команда	Описание
Обновить ПО	Выполняется обновление установленной ранее версии программного обеспечения клиента на новую. В этом случае для задания настраивается параметр "Время ожидания перезагрузки ..." и указывается версия клиента для обновления. Запуск процесса обновления программного обеспечения на выбранных компьютерах происходит при выходе пользователя из системы
Исправить ПО	Выполняется исправление установленного ранее программного обеспечения клиента. При выборе этой команды на экране появится сообщение о сформированном задании. Запуск процесса исправления программного обеспечения на выбранных компьютерах происходит при их перезагрузке
Удалить ПО	Выполняется удаление установленного программного обеспечения клиента. При выборе этой команды на экране появится сообщение о сформированном задании. Запуск процесса удаления программного обеспечения на выбранных компьютерах происходит автоматически
Установить пакет исправлений	Выполняется установка пакетов обновлений. В этом случае в параметрах задания можно выбрать один или несколько пакетов обновлений, ранее загруженных в репозиторий. Если пакет обновлений уже установлен, то он не появится в параметрах задания. При выборе единого пакета обновлений выполняется установка кумулятивных пакетов обновлений, входящих в состав единого пакета. В отличие от обычных пакетов обновлений, единый пакет всегда присутствует в параметрах задания. При повторном запуске установки появится уведомление, что единый пакет уже установлен. Запуск процесса установки пакетов обновлений на выбранных компьютерах происходит при их перезагрузке
Удалить все пакеты исправлений	Удаляет все установленные ранее пакеты обновлений. При выборе этой команды на экране появится сообщение о сформированном задании. Запуск процесса удаления обновлений на выбранных компьютерах происходит при их перезагрузке

В правой части окна появится панель настройки параметров задания.



5. Настройте параметры задания и нажмите кнопку "Установить" в нижней части панели. Для задания на установку ПО клиента выполняется настройка следующих параметров:
   - версия устанавливаемого ПО;
   - папка для установки ПО;
   - время ожидания перезагрузки компьютера после установки — если выбран вариант "Не ограничено", автоматическая перезагрузка компьютера после установки ПО не выполняется. Для включения режима автоматической перезагрузки выберите вариант "Задать время" и в поле ввода укажите, через сколько минут после завершения установки следует выполнить автоматическую перезагрузку;

     Пояснение. При настройке параметров задания для обновления ПО данный параметр определяет, через сколько минут после получения задания компьютер автоматически перезагрузится. Обновление ПО будет выполнено во время перезагрузки компьютера.
   - параметры — определяет параметры командной строки, с которыми будет запущена программа установки (опционально);
   - лицензии на использование компонентов;
   - пакеты обновлений;
   - учетные данные локального администратора (доменного пользователя, входящего в локальные группы администраторов на выбранных компьютерах, а также обладающего привилегией интерактивного входа в систему).
6. После создания задания перейдите к списку заданий на вкладке "Задания" для проверки добавления нового элемента.



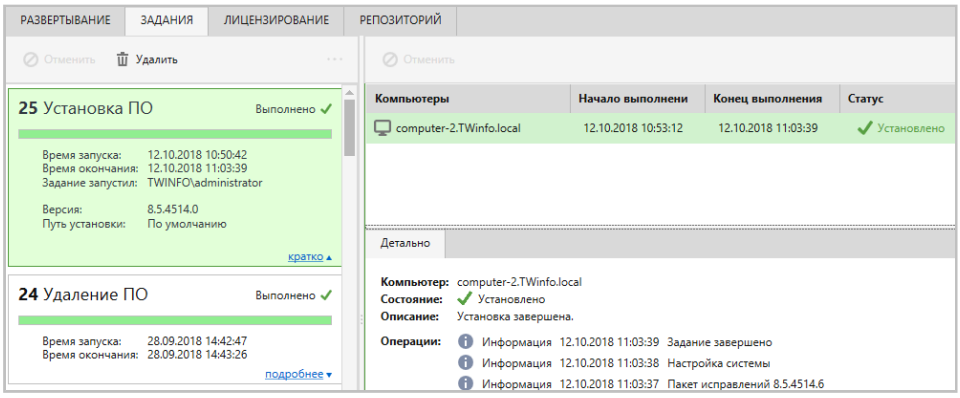
Контроль выполнения заданий

Сформированные задания применяются на компьютерах в соответствии с заданными параметрами. Администратор может контролировать процесс развертывания ПО с помощью списка заданий.

Для контроля выполнения заданий:

1. В панели "Развертывание" перейдите на вкладку "Задания".

   Пример содержимого вкладки представлен на рисунке ниже.



   Для заданий и компьютеров выводятся сведения о времени и статусе выполнения процессов.

2. Для вывода дополнительных сведений о задании нажмите кнопку "Подробнее" в нижней части информационного блока. Для просмотра подробных сведений о компьютере можно включить отображение области сведений с помощью кнопки, которая расположена в правой части строки под списком компьютеров.

Примечание. Если для нормально функционирующего компьютера статус ожидания запуска процесса сохраняется длительное время, проверьте соответствие компьютера требованиям к аппаратному и программному обеспечению для установки клиента (см. стр.45). Например, выполнение задания возможно при условии, что на компьютере разрешено использование портов для доступа к общим ресурсам: 137, 138, 139, 445. Данные порты по умолчанию закрыты брандмауэром при отсутствии на компьютере сетевых папок общего доступа. Для разрешения использования указанных портов можно изменить параметры брандмауэра или создать произвольную папку и открыть к ней общий доступ.

3. При необходимости отменить выполнение задания:
   - чтобы отменить выполнение на всех компьютерах, к которым относится задание, — выберите его и нажмите кнопку "Отменить", которая расположена над списком заданий в разделе "Задание";
   - чтобы отменить выполнение на отдельных компьютерах — выберите их в списке и нажмите кнопку "Отменить", которая расположена над списком компьютеров в разделе "Компьютер".

Внимание! Отменить задание можно только до его выполнения. Если нажать кнопку "Отмена" в процессе выполнения задания, задание будет отмечено как отмененное, но его выполнение не остановится.

4. После завершения выполнения задания его можно удалить из списка. Для этого выберите его и нажмите кнопку "Удалить", которая расположена над списком заданий в разделе "Задание".

Установка с использованием групповых политик

Реализация автоматической установки и обновления ПО клиента с использованием групповых политик основана на применении специально настроенных групповых политик на компьютерах определенных организационных подразделений. На каждом компьютере запуск процесса установки или обновления происходит автоматически при его перезагрузке. Если ПО клиента на компьютере не установлено — запускается процесс установки. При наличии ПО клиента — выполняется обновление на текущую версию.

Процедура настройки системы для автоматической установки и обновления состоит из следующих этапов:

1. Начальное формирование структуры ОУ (см. стр.73).
2. Создание файлов со сценарием установки (см. стр.74).
3. Создание общедоступного сетевого ресурса (см. стр.79).
4. Создание организационных подразделений и включение в них компьютеров (см. стр.79).
5. Создание и настройка групповых политик для нужных организационных подразделений (см. стр.80).

Начальное формирование структуры ОУ

Компьютеры, на которых будет выполняться автоматическая установка ПО клиента (сетевой режим работы), следует включить в структуру оперативного управления (ОУ), подчинив каждый компьютер серверу безопасности. Для этого в системе должна быть развернута соответствующая структура серверов безопасности и подготовлено рабочее место администратора Secret Net Studio.

Подчинение серверам безопасности компьютеров без установленного клиентского ПО осуществляется средствами Центра управления.

Примечание. Не требуется подчинять серверу безопасности компьютеры, на которых предполагается использовать клиент Secret Net Studio в автономном режиме работы.

Создание файлов со сценарием установки

Сценарий предназначен для автоматизации процесса установки клиентского ПО и позволяет полностью автоматизировать ввод информации, запрашиваемой программой установки клиента.

Файлы со сценарием установки создаются в INI-формате и являются файлами конфигурации, которые содержат данные по настройке клиентского ПО Secret Net Studio. Созданные файлы необходимо поместить в корневые папки созданных ОСР (см. стр.**79**).

Создать файл сценария можно средствами программы установки клиента (см. стр.**60**) или вручную.

Совет. В качестве шаблона сценария можно использовать файл сценария, созданный с помощью программы установки клиента, или использовать пример сценария, приведенный ниже.

Для создания файла сценария вручную:

- В текстовом редакторе создайте файл SnInst.rsp, сформируйте его содержимое и сохраните файл.

Структура файла сценария

Файл сценария имеет следующую структуру:

[Section_1]

параметр_1 = значение_параметра_1

параметр_2 = значение_параметра_2

...

параметр_N = значение_параметра_N

[Section_2]

параметр_1 = значение_параметра_1

параметр_2 = значение_параметра_2

...

параметр_N = значение_параметра_N

[Section_N]

параметр_1 = значение_параметра_1

параметр_2 = значение_параметра_2

...

параметр_N = значение_параметра_N

В секциях [Section...] указываются параметры и их значения, необходимые программе установки ПО клиента. Перечень основных секций и параметров представлен в следующей таблице.

Параметр	Значение по умолчанию	Описание
Секция [Core]		
Action	install	Определяет состояние компонента "Базовая защита": • "install" – компонент установлен; • "none" – компонент не установлен
Секция [Console]		
Action	install	Определяет состояние Локального центра управления: • "install" – программа установлена; • "none" – программа не установлена

Параметр	Значение по умолчанию	Описание
Секция [Local]		
Action	none	Определяет состояние компонента локальной защиты: • "install" – компонент установлен; • "none" – компонент не установлен
ERASER	0	Определяет состояние компонента "Затирание данных": • "1" — компонент включен; • "0" — компонент отключен
DC	0	Определяет состояние компонента "Контроль устройств": • "1" — компонент включен; • "0" — компонент отключен
FDC	0	Определяет состояние компонента "Дискреционное управление доступом": • "1" — компонент включен; • "0" — компонент отключен
EXEQUOTA	0	Определяет состояние компонента "Замкнутая программная среда": • "1" — компонент включен; • "0" — компонент отключен
MC	0	Определяет состояние компонента "Полномочное управление доступом": • "1" — компонент включен; • "0" — компонент отключен
Секция [Pc]		
Action	none	Определяет состояние компонента "Контроль печати": • "install" – компонент включен; • "none" – компонент отключен
Секция [Disk]		
Action	none	Определяет состояние компонента "Защита дисков и шифрование данных": • "install" – компонент включен; • "none" – компонент отключен
FDE	0	Определяет состояние компонента полнодискового шифрования: • "1" — компонент установлен; • "0" — компонент не установлен
CRCONT	0	Определяет состояние компонента защиты дисков и защиты криптоконтейнеров: • "1" — компонент установлен; • "0" — компонент не установлен
Секция [Ta]		
Action	none	Определяет состояние компонента сетевой защиты: • "install" – компонент установлен; • "none" – компонент не установлен
TA_Firewall	0	Определяет состояние компонента "Персональный межсетевой экран": • "1" — компонент включен; • "0" — компонент отключен

Параметр	Значение по умолчанию	Описание
TA_IPSEC	0	Определяет состояние компонента "Авторизация сетевых соединений": • "1" — компонент включен; • "0" — компонент отключен
Секция [Common]		
Installdir	[ProgramFilesFolder]Secret Net Studio\Client	Папка установки ПО клиента
User	Отсутствует	Имя пользователя из группы администраторов домена безопасности
Password	Отсутствует	Пароль пользователя
Server	Отсутствует	Идентификатор безопасности сервера безопасности: • присутствует – сетевой режим функционирования клиента; • отсутствует – автономный режим функционирования клиента
Source *	Отсутствует	Источник установочного файла клиента
Division	Отсутствует	Учетная информация компьютера: название подразделения
SysName	Отсутствует	Учетная информация компьютера: название автоматизированной системы
Workplace	Отсутствует	Учетная информация компьютера: рабочее место
Id	Отсутствует	Учетная информация компьютера: номер системного блока
LicenseFilePath *	Отсутствует	Имя файла лицензии
Servername	Отсутствует	DNS-имя сервера безопасности
locale **	Отсутствует	Определяет язык системы: • "ru-RU" – русский; • "en-US" – английский
RebootTimeOut	Отсутствует	Время в минутах до перезагрузки компьютера и начала установки
Секция [Softpspt]		
Action	none	Определяет состояние компонента "Паспорт ПО": • "install" – компонент включен; • "none" – компонент отключен
Секция [Patches]		
Count	Отсутствует	Количество необязательных (Normal) пакетов исправлений для установки
PatchN	Отсутствует	Путь к необязательному пакету исправлений, где "N" – порядковый номер пакета
Секция [Te]		
Action	none	Определяет состояние компонента "Доверенная среда": • "install" – компонент включен; • "none" – компонент отключен

* Обязательный параметр.

** Обязательный и регистрозависимый параметр.

Для задания пути допускается использование переменных среды. Имя переменной среды задается в квадратных скобках и должно находиться в начале значения параметра. Перечень поддерживаемых переменных среды представлен в таблице.

Переменная среды	Пример значения
WindowsVolume	C:\
WindowsFolder	C:\WINDOWS\
USERPROFILE	C:\Documents and Settings\Ivanov\
TemplateFolder	C:\Documents and Settings\All Users\Templates\
TempFolder	C:\Documents and Settings\Ivanov\Local Settings\Temp
SystemFolder	C:\WINDOWS\system32\
StartupFolder	C:\Documents and Settings\All Users\Start Menu\Programs\Startup\
StartMenuFolder	C:\Documents and Settings\All Users\Start Menu
SendToFolder	C:\Documents and Settings\Ivanov\SendTo\
ProgramMenuFolder	C:\Documents and Settings\All Users\Start Menu\Programs\
PrimaryVolumePath	C:\
PersonalFolder	C:\Documents and Settings\Ivanov\My Documents\
MyPicturesFolder	C:\Documents and Settings\Ivanov\My Documents\My Pictures\
LocalAppDataFolder	C:\Documents and Settings\Ivanov\Local Settings\Application Data\
FontsFolder	C:\WINDOWS\Fonts\
FavoritesFolder	C:\Documents and Settings\Ivanov\Favorites\
CommonFilesFolder	C:\Program Files\Common Files\
CommonAppDataFolder	C:\Documents and Settings\All Users\Application Data\
ProgramFilesFolder	C:\Program Files\
AppDataFolder	C:\Documents and Settings\Ivanov\Application Data
AdminToolsFolder	C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\
ALLUSERSPROFILE	C:\Documents and Settings\All Users

Пример содержимого файла сценария

Ниже представлен пример содержимого файла сценария для установки клиента, который будет функционировать в автономном режиме.

```
[core]
Action=install
[console]
Action=install
[local]
Action=install
ERASER=1
DC=1
FDC=1
EXEQUOTA=1
MC=1
[pc]
Action=none
[disk]
Action=install
```

```
FDE=1
CRCONT=1
[ta]
Action=install
TA_Firewall=1
TA_IPSEC=1
[Common]
Installdir=C:\Program Files\Secret Net Studio\Client\
server=
Source=\\computer.TWinfo.local\OSR
LicenseFilePath=full_new
locale=ru-RU
[softpspt]
Action=none
[patches]
count=2
patch0=\\computer.TWinfo.local\OSR\tools\SecurityCode\Patches\8_ 5_ 5329_ 8_ Inc72574_Build5\
patch1=\\computer.TWinfo.local\OSR\tools\SecurityCode\Patches\8_ 5_ 5329_ 9_ Inc72994_Build6\
```

В приведенном примере предписывается:

1. Установить компонент "Базовая защита".
2. Установить Локальный центр управления.
3. Установить компонент локальной защиты.
   - Включить компонент "Затирание данных".
   - Включить компонент "Контроль устройств".
   - Включить компонент "Дискреционное управление доступом".
   - Включить компонент "Замкнутая программная среда".
   - Включить компонент "Полномочное управление доступом".
4. Отключить компонент "Контроль печати".
5. Включить компонент "Защита дисков и шифрование данных".
   - Установить компонент защиты дисков.
   - Установить компонент защиты криптоконтейнеров.
   - Установить компонент полнодисокового шифрования.
6. Установить компонент сетевой защиты.
   - Включить компонент "Персональный межсетевой экран".
   - Включить компонент "Авторизация сетевых соединений".
7. Установить продукт в папку программ на системном диске в папке \Secret Net Studio\Client.
   - Идентификатор безопасности сервера безопасности отсутствует.
   - Источник установочного файла клиента:\\computer.TWinfo.local\OSR.
   - Имя файла используемой лицензии "full_new".
   - Установить русский язык для системы защиты.
8. Отключить компонент "Паспорт ПО".
9. Установить два необязательных (Normal) пакета обновлений. Все обязательные (Critical) пакеты обновлений устанавливаются автоматически.
   - Два пакета обновлений с указанием их месторасположения.

Создание общедоступного сетевого ресурса

В домене AD необходимо создать ОСР, содержащий файлы для установки ПО клиента, файл с лицензиями и файл со сценарием установки.

Внимание! Если в домене AD имеется несколько серверов безопасности, то для каждого из них требуется создать отдельный ОСР со своим набором данных.

Для создания ОСР:

1. На одном из компьютеров домена создайте папку и откройте к ней общий доступ.

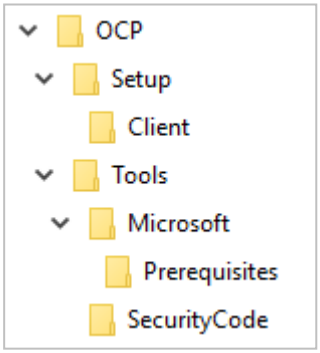
   Внимание! Дополнительно предоставьте права доступа на чтение содержимого этой папки всем учетным записям компьютеров, на которые планируется устанавливать ПО клиента, или группе "Domain Computers".

   Примечание. Во время проведения автоматической установки ПО этот компьютер должен быть доступен для сетевых обращений. Рекомендуется создать ОСР на одном из файловых серверов домена.

2. С установочного диска Secret Net Studio скопируйте в созданную папку содержимое следующих папок (сохраняя их структурную вложенность):

Имя папки	Назначение
\Setup\Client\	Содержит дистрибутивы для установки ПО клиента на 32- и 64-разрядных версиях ОС Windows
\Tools\Microsoft\Prerequisites	Содержит файлы установки необходимых обновлений ОС Windows. Если файлы отсутствуют, автоматическая установка клиента на компьютерах не будет выполняться
\Tools\SecurityCode\	Содержит вспомогательные утилиты и файлы настройки, необходимые для работы с Secret Net Studio

   Структура папки ОСР представлена на следующем рисунке.



3. В созданную папку скопируйте файл с лицензиями на использование компонентов Secret Net Studio.

   Совет. Если предполагается использовать клиент в сетевом режиме работы, также добавьте на сервер безопасности лицензии, содержащиеся в данном файле.

4. В созданную папку скопируйте файл со сценарием установки.

Настройка Active Directory

Формирование организационных подразделений

Чтобы выделить компьютеры домена, на которых будет выполняться автоматическая установка или обновление ПО, необходимо создать организационные подразделения (Organizational Units) и включить в них нужные компьютеры. Также можно использовать имеющиеся организационные подразделения.

Создание организационных подразделений и добавление объектов осуществляется стандартными средствами управления.

Создание и настройка групповых политик

Для подготовленных организационных подразделений необходимо создать групповые политики автоматической установки ПО. Групповые политики создаются отдельно для 32- и 64-разрядных версий ОС Windows.

После того как автоматическая установка ПО будет выполнена на всех компьютерах, созданные групповые политики можно удалить стандартными способами.

Для создания групповой политики на контроллере домена:

1. Вызовите консоль "Управление групповой политикой".
2. Вызовите контекстное меню организационного подразделения, на компьютерах которого будет проводиться автоматическая установка, и выберите команду "Создать объект групповой политики в этом домене и связать его".
3. В появившемся диалоге введите имя создаваемой политики и нажмите кнопку "ОК".

   Новая политика появится в иерархическом списке в качестве подчиненного объекта организационного подразделения.
4. Вызовите контекстное меню политики и выберите команду "Изменить".

   На экране появится окно редактора групповых политик.
5. В дереве объектов политики перейдите к разделу "Конфигурация компьютера\ Политики\Конфигурация программ\Установка программ", вызовите контекстное меню подраздела и выберите команду "Создать\Пакет".

   На экране появится диалог "Открытие".
6. В поле "Имя файла" введите нужное значение:
   - для применения политики на компьютерах с 32-разрядной ОС Windows: <*сетевой_путь_к_папке_ОСР*>\Setup\Client\Win32\InstAgent.msi;
   - для применения политики на компьютерах с 64-разрядной ОС Windows: <*сетевой_путь_к_папке_ОСР*>\Setup\Client\x64\InstAgent.msi.
7. В диалоговом окне нажмите кнопку "Открыть".

   На экране появится окно развертывания программ.
8. Нажмите кнопку "ОК".

Совет. Для созданного пакета с 32-разрядной версией дистрибутива рекомендуется удалить отметку из поля "Сделать это 32-разрядное X86 приложение доступным для компьютеров с архитектурой Win64". Для этого в свойствах пакета перейдите на вкладку "Развертывание " и нажмите кнопку "Дополнительно".

Совет. Если используются несколько организационных подразделений для автоматической установки ПО, создавать отдельные групповые политики для каждого подразделения необязательно. В остальных подразделениях можно добавить ссылку на созданные групповые политики (с помощью команды контекстного меню "Связать существующий объект групповой политики").

Для применения созданной групповой политики:

1. Перезагрузите компьютер, на котором выполняется установка ПО клиента.
2. Войдите в систему под учетной записью пользователя.

   После успешного входа пользователя в систему над пиктограммой Secret Net Studio, находящейся на панели задач Windows, появится сообщение об установке. После запуска перезагрузки компьютера начнется установка компонентов Secret Net Studio.

Установка с использованием SCCM

Реализация централизованного запуска процессов для клиентов Secret Net Studio – C осуществляется с помощью продукта для управления ИТ- инфраструктурой на основе Microsoft Windows и смежных устройств (SCCM).

Средствами SCCM может происходить запуск процессов:

- установки, обновления, исправления или удаления клиентского ПО;
- установки или удаления пакетов обновлений.

Процедура настройки системы состоит из следующих этапов:

1. Начальное формирование структуры ОУ (см. стр.**81**).
2. Создание файлов со сценарием установки (см. стр.**81**).
3. Создание общедоступного сетевого ресурса SCCM (см. стр.**83**).
4. Настройка SCCM (см. стр.**83**).

Начальное формирование структуры ОУ

Компьютеры, на которых будет выполняться запуск процессов, следует подчинить серверу безопасности. Для этого в системе должна быть развернута соответствующая структура серверов безопасности и подготовлено рабочее место администратора Secret Net Studio.

Подчинение серверам безопасности компьютеров без установленного клиентского ПО осуществляется средствами Центра управления.

Примечание. Не требуется подчинять серверу безопасности компьютеры, на которых предполагается использовать клиент Secret Net Studio в автономном режиме работы.

Создание файлов со сценарием установки

Описание процесса создания файлов со сценарием для процесса установки ПО клиента и структура файла сценария соответствует описанию групповых политик (стр.**74**).

Пример содержимого файла сценария

Ниже представлен пример содержимого файла сценария для установки клиента, который будет функционировать в сетевом режиме.

[core]
Action=install
[console]
Action=install
[local]
Action=install
ERASER=1
DC=1
FDC=1
EXEQUOTA=1
MC=1
[pc]
Action=install
[disk]
Action=install
FDE=1
CRCONT=1
[Common]
Action=install
Installdir=C:\Program Files\Secret Net Studio\Client
server=S-1-5-21-3534210826-639358159-2414785253-3826
Source=\\MSS2012\OSR
LicenseFilePath=lic

servername=WIN-ATC89VIN2B9.testsn7.ru

locale=ru-RU

[ta]

Action=install

TA_Firewall=1

TA_IPSEC=1

TA_IDS=1

[softpspt]

Action=none

[te]

Action=none

[antivirus]

Action=install

[patches]

count=3

patch0=\\MSS2012\OSR\tools\SecurityCode\Patches\8_6_6186_11_IncidentTest_LocalControlCentre_Client

patch1=\\MSS2012\OSR\tools\SecurityCode\Patches\8_6_6186_14_IncidentTest_AuthServer_Server

patch2=\\MSS2012\OSR\tools\SecurityCode\Patches\8_ 6_ 6186_ 16_ IncidentTest5_Core_Client

В приведенном примере предписывается:

1. Установить компонент "Базовая защита".
2. Установить Локальный центр управления.
3. Установить компонент локальной защиты.
   - Включить компонент "Затирание данных".
   - Включить компонент "Контроль устройств".
   - Включить компонент "Дискреционное управление доступом".
   - Включить компонент "Замкнутая программная среда".
   - Включить компонент "Полномочное управление доступом".
4. Включить компонент "Контроль печати".
5. Включить компонент "Защита дисков и шифрование данных".
   - Установить компонент защиты дисков.
   - Установить компонент защиты криптоконтейнеров.
   - Установить компонент полнодискового шифрования.
6. Установить продукт в папку программ на системном диске в папке \Secret Net Studio\Client.
   - Идентификатор безопасности сервера безопасности S- 1- 5- 21- 3534210826-639358159-2414785253-3826.
   - Источник установочного файла клиента:\\MSS2012\OSR.
   - Имя файла используемой лицензии "lic".
   - DNS-Имя сервера безопасности WIN-ATC89VIN2B9.testsn7.ru.
   - Установить русский язык для системы защиты.
7. Установить компонент сетевой защиты.
   - Включить компонент "Персональный межсетевой экран".
   - Включить компонент "Авторизация сетевых соединений".
8. Отключить компонент "Паспорт ПО".
9. Отключить компонент "Доверенная среда".

10. Установить три необязательных (Normal) пакета обновлений. Все обязательные (Critical) пакеты обновлений устанавливаются автоматически.
    - Три пакета обновлений с указанием их месторасположения.

Создание общедоступного сетевого ресурса SCCM

В домене AD необходимо создать ОСР, содержащий файлы для установки ПО клиента, файл с лицензиями и файл со сценарием установки.

Внимание! Если в домене AD имеется несколько серверов безопасности, то для каждого из них требуется создать отдельный ОСР со своим набором данных.

Для создания ОСР:

1. На одном из компьютеров домена создайте папку и откройте общий доступ к ней и к диску, на котором расположена эта папка. Дополнительно предоставьте все права доступа на содержимое этой папки всем учетным записям компьютеров, на которые планируется устанавливать ПО клиента.

   Примечание. Во время проведения автоматической установки ПО этот компьютер должен быть доступен для сетевых обращений. Рекомендуется создать ОСР на одном из файловых серверов домена.

2. В созданную папку скопируйте файл с лицензиями на использование компонентов Secret Net Studio.

   Совет. Если предполагается использовать клиент в сетевом режиме работы, также добавьте на сервер безопасности лицензии, содержащиеся в данном файле.

3. В созданную папку скопируйте файл со сценарием установки.

   Примечание. Для обновления, исправления, удаления клиентского ПО и удаления пакетов обновлений наличие файла с лицензиями на использование компонентов и файла со сценарием установки не требуется в ОСР.

Настройка SCCM

Возможны следующие варианты развертывания ПО на клиентском компьютере:

- пакет установки (см. ниже);
- приложение (см. стр.**89**).

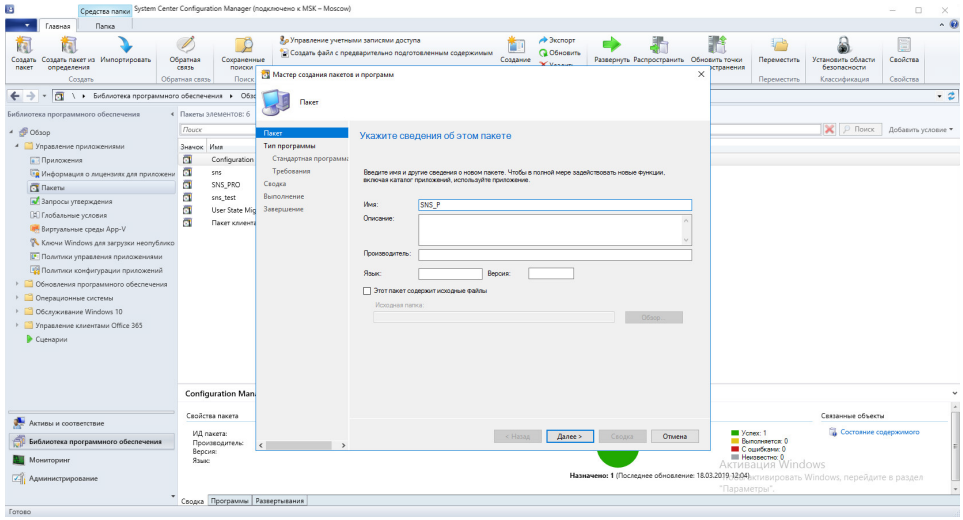
Развертывание пакета установки через SCCM

Для централизованного развертывания клиентов необходимо создать и установить пакет установки.

Для создания пакета установки:

1. Откройте System Center Configuration Manager.
2. В нижней части панели навигации выберите "Библиотека программного обеспечения" (слева в основном окне).
3. В верхней части панели навигации в окне структуры раскройте ветвь "Управление приложениями" (слева в основном окне).
4. Вызовите контекстное меню объекта "Пакеты" и выберите команду "Создать пакет".

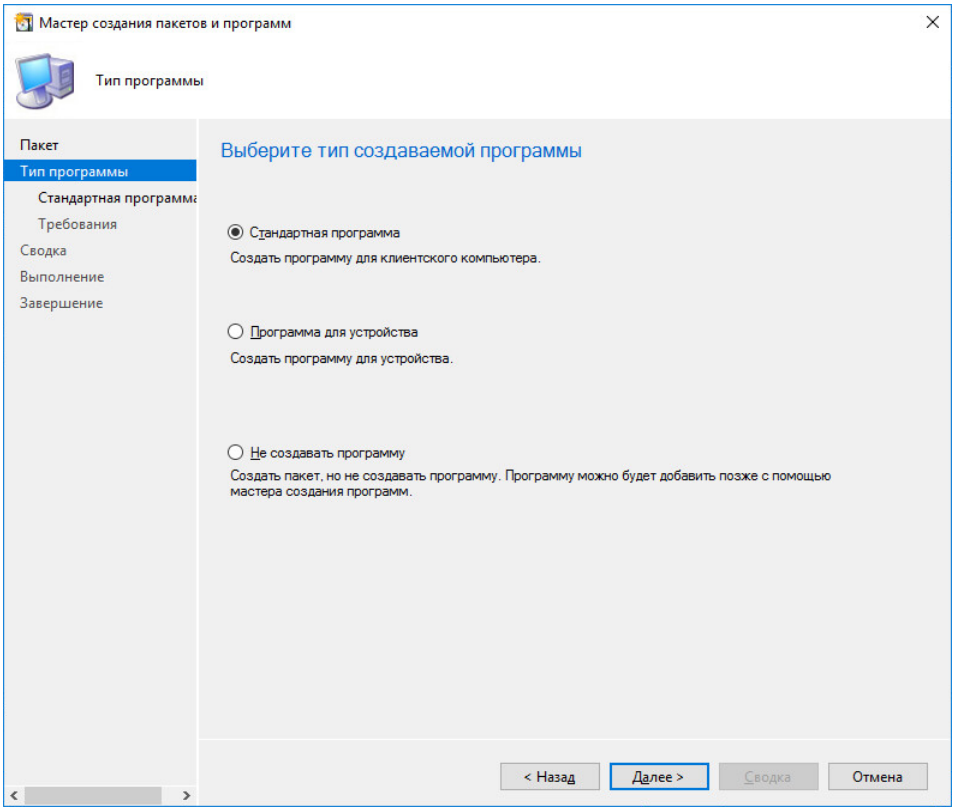
   На экране появится диалог, подобный следующему.



5. В поле "Имя" укажите название пакета и нажмите кнопку "Далее >".

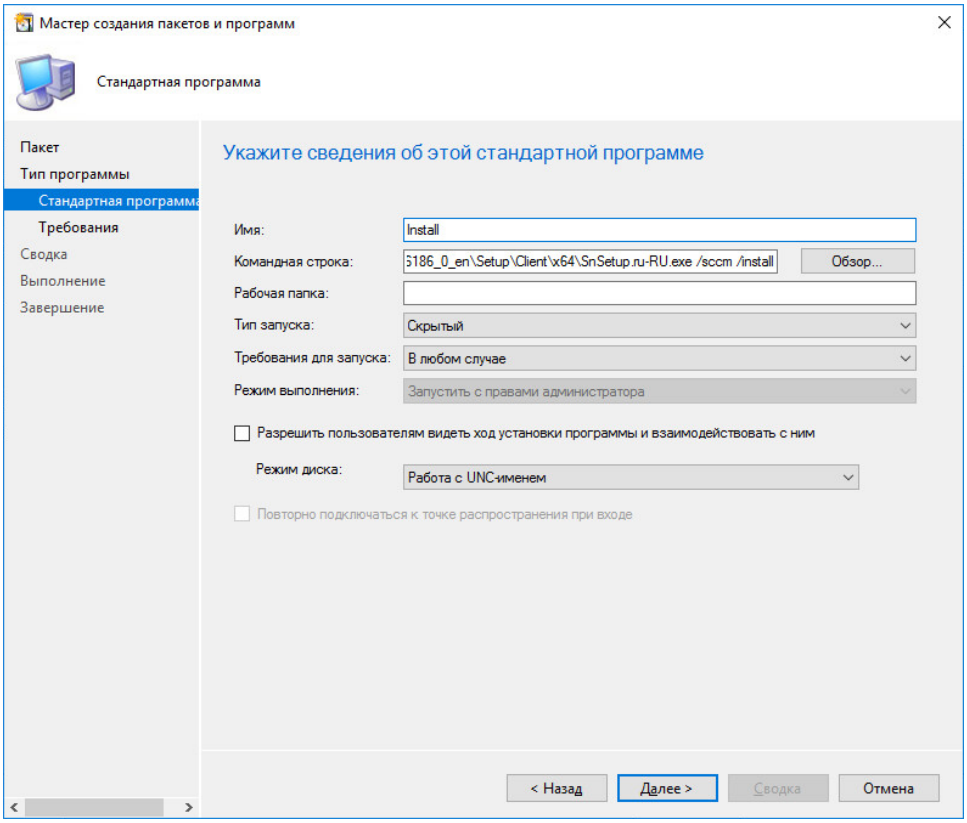
Примечание. Если дистрибутив находится на ОСР, то не требуется устанавливать отметку в поле "Этот пакет содержит исходные файлы".

На экране появится диалог, подобный следующему.



6. В диалоге установите отметку в поле "Стандартная программа" и нажмите кнопку "Далее >".

На экране появится диалог, подобный следующему.



7. Для стандартной программы выполните следующие действия:

- Укажите информацию:
  - в поле "Имя" укажите название стандартной программы;
  - в поле "Командная строка" укажите в соответствующем формате путь к дистрибутиву и команду (см. ниже);
  - в поле "Тип запуска" выберите параметр "Скрытый";
  - в поле "Требования для запуска" выберите параметр "В любом случае".
- Нажмите кнопку "Далее >".

На экране появится диалог требований для стандартной программы.

Поле "Командная строка" имеет следующий формат ввода:

```
<путь к дистрибутиву> /sccm /<команда>
```

Описание команд представлено в следующей таблице.

Команда	Описание
install [/timeout:x]	Выполняется установка программного обеспечения клиента. Необязательный параметр *timeout:x* — время в минутах до перезагрузки компьютера и начала установки. По умолчанию это время составляет 720 минут (12 часов)
upgrade	Выполняется обновление установленной ранее версии программного обеспечения клиента на новую
repair	Выполняется исправление установленного ранее программного обеспечения клиента
uninstall	Выполняется удаление установленного программного обеспечения клиента
applypatch "путь к папке с пакетом обновлений"	Выполняется установка пакетов обновлений
removeallpatches	Удаляет все установленные ранее пакеты обновлений

8. Нажмите кнопку "Далее >".

   На экране появится диалог подтверждения параметров.

9. В диалоге проверьте содержимое и нажмите кнопку "Далее >".

   Начнется процесс создания пакета установки.

10. После завершения нажмите кнопку "Закрыть".

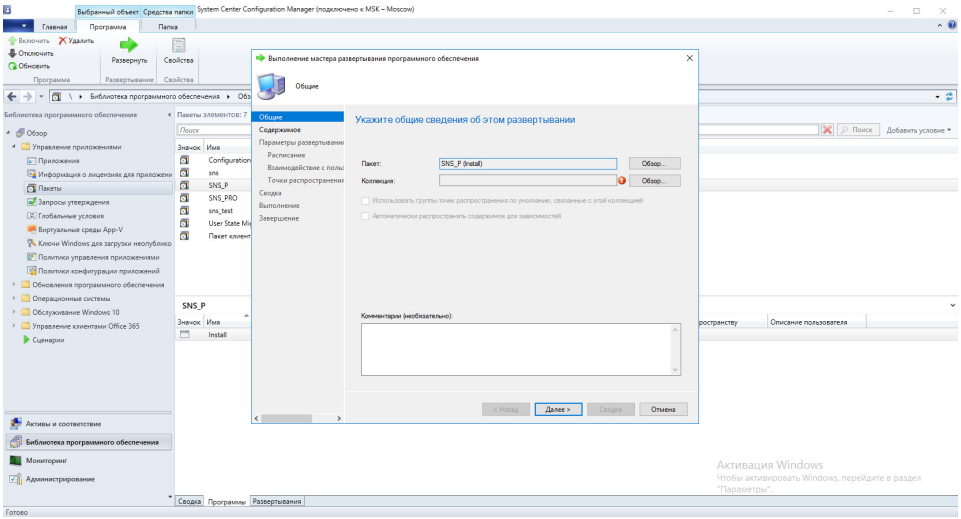
    По окончании процесса в списке пакетов установок появится новый пакет, содержащий сведения о созданных программах.

Примечание. Добавление новых стандартных программ в пакет установки осуществляется после его создания. Для добавления новой стандартной программы вызовите контекстное меню созданного пакета установки и выберите команду "Создать программу", а затем выполните действия **6–10**.

Для установки стандартной программы созданного пакета установки:

1. Откройте System Center Configuration Manager.
2. В нижней части панели навигации выберите "Библиотека программного обеспечения" (слева в основном окне).
3. В верхней части панели навигации в окне структуры раскройте ветвь "Управление приложениями" (слева в основном окне).
4. Выберите объект "Пакеты".
5. В списке пакетов установок выберите созданный ранее пакет.
6. Перейдите на вкладку "Программы" (снизу в основном окне) и выберите стандартную программу, созданную ранее.
7. Вызовите контекстное меню стандартной программы и выберите команду "Развернуть".

   На экране появится диалог, подобный следующему.



8. Напротив поля "Коллекция" нажмите кнопку "Обзор" и в появившемся списке выберите необходимую коллекцию компьютеров, на которую требуется установить пакет установки, а затем нажмите кнопку "OK".
9. Нажмите кнопку "Далее >".

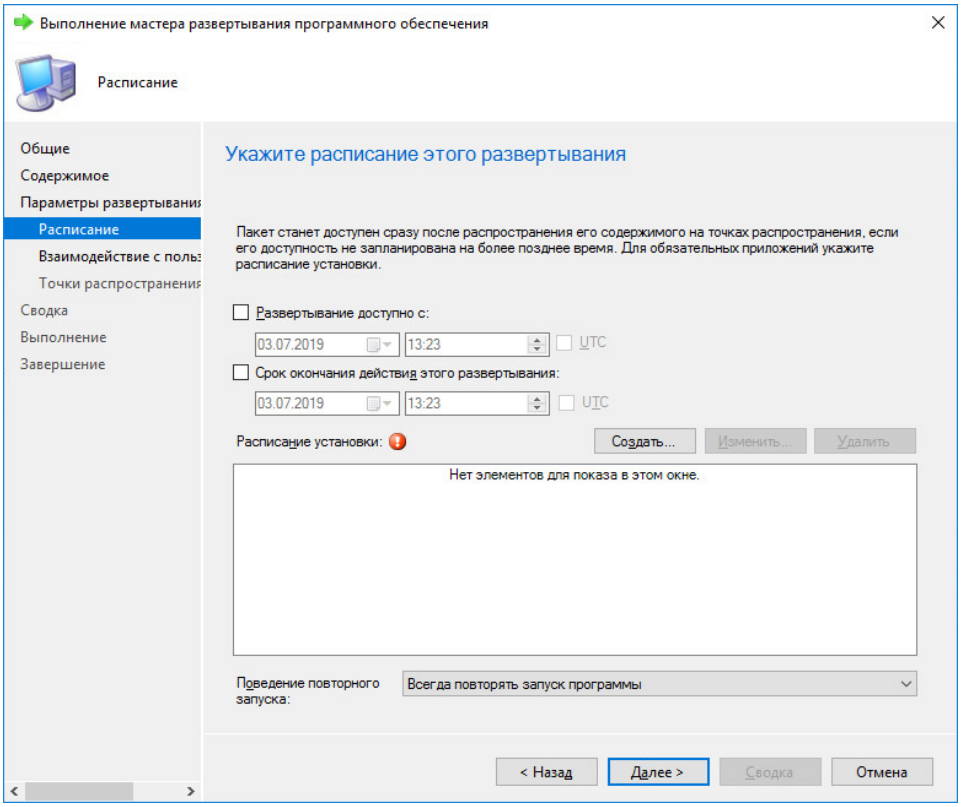
   На экране появится диалог места распространения содержимого.

10. Нажмите кнопку "Далее >".

    На экране появится диалог параметров управления процессом развертывания этого программного обеспечения.

11. В поле "Намерение" укажите "Обязательная установка" и нажмите кнопку "Далее >".

    На экране появится диалог расписания развертывания этого программного обеспечения.



12. Выполните следующие действия:

- Нажмите кнопку "Создать":
  - Установите отметку в поле "Назначить сразу после этого события";
  - В выпадающем меню выберите "Как можно скорее".
- Нажмите кнопку "ОК".

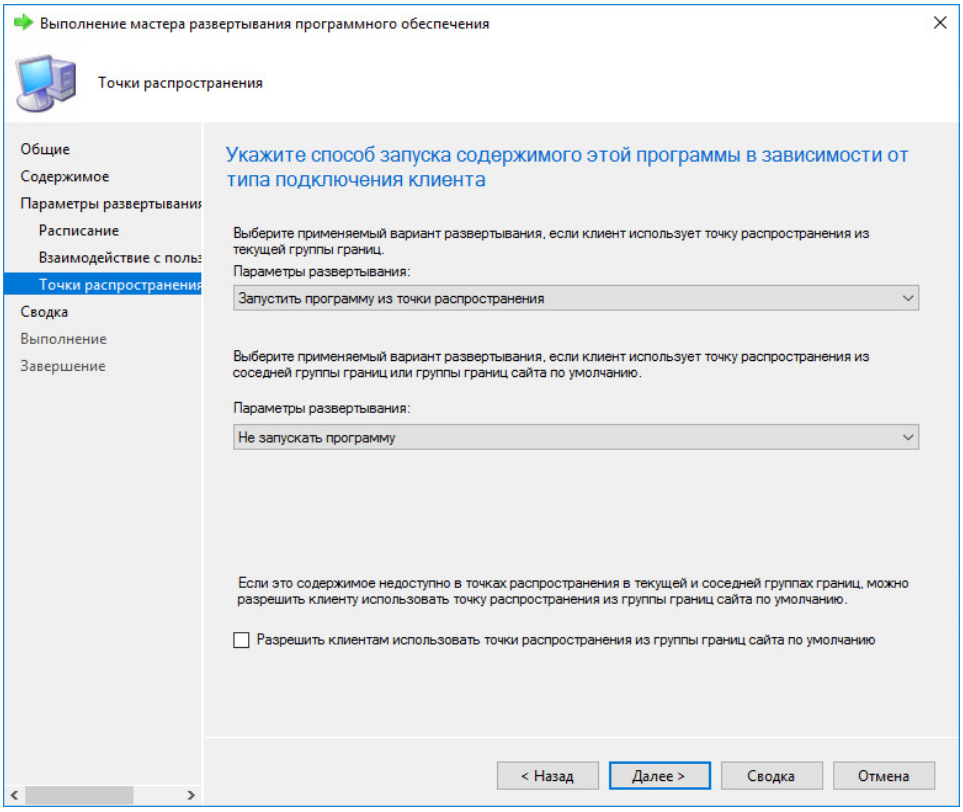
В списке расписания заданий появится новая запись.

13. В поле "Поведение повторного запуска" выберите "Всегда повторять запуск программы" и нажмите кнопку "Далее >".

На экране появится диалог параметров взаимодействия с пользователем при установке этого программного обеспечения.

14. Нажмите кнопку "Далее >".

На экране появится диалог, подобный следующему.



15. В поле "Параметры развертывания" укажите "Запустить программу из точки распространения" и нажмите кнопку "Далее >".

На экране появится диалог подтверждения параметров развертывания.

16. В диалоге проверьте содержимое и нажмите кнопку "Далее >".

Начнется процесс установки стандартной программы.

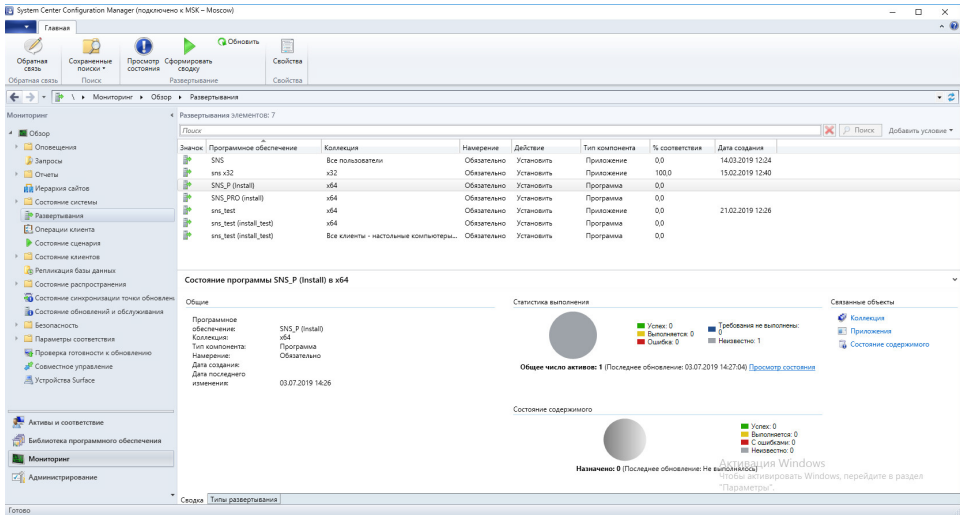
17. После завершения нажмите кнопку "Закрыть".

Примечание. Для установки созданных ранее стандартных программ из пакета установки выполните действия **6–17**.

Для отслеживания процесса выполнения стандартной программы:

1. Откройте System Center Configuration Manager.
2. В нижней части панели навигации выберите "Мониторинг" (снизу в основном окне).
3. В верхней части панели навигации в окне структуры выберите "Развертывания".

   На экране появится диалог, подобный следующему.



4. В списке программного обеспечения выберите требуемую стандартную программу и посмотрите ее состояние.

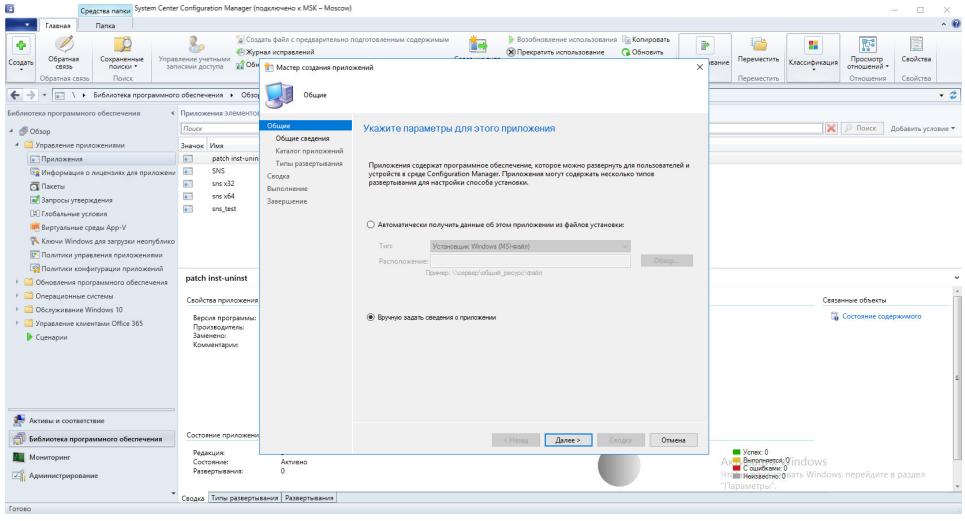
Развертывание приложения через SCCM

Для централизованного развертывания клиентов необходимо создать и установить приложение.

Для создания приложения:

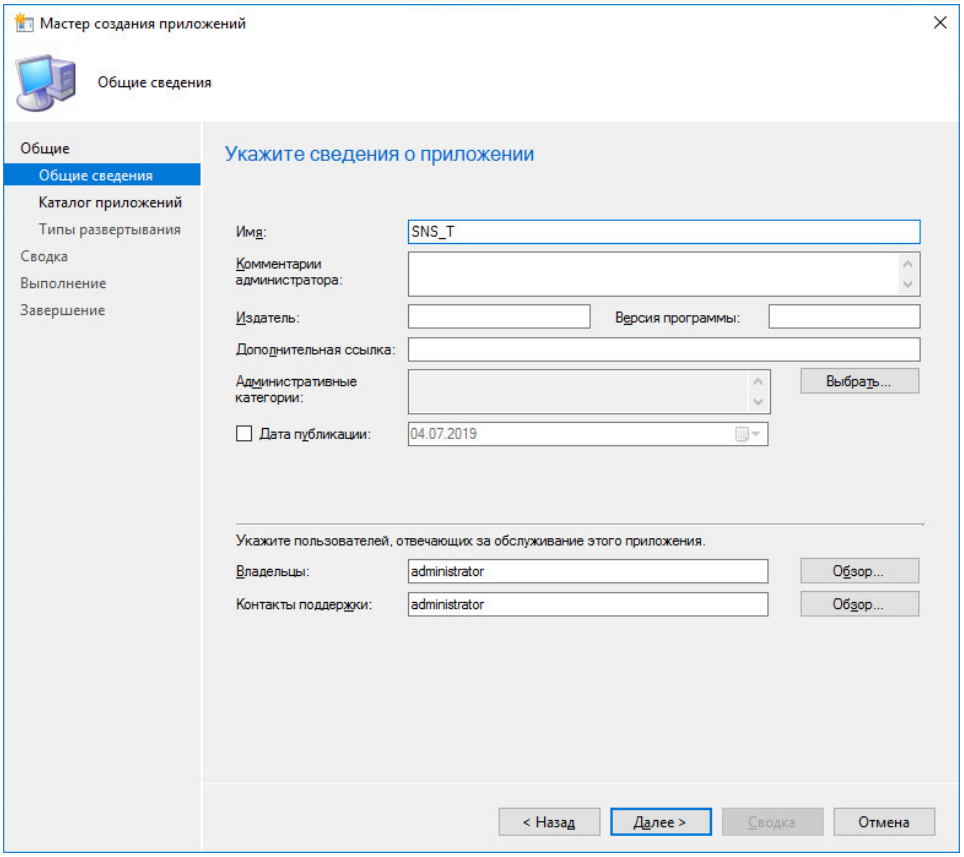
1. Откройте System Center Configuration Manager.
2. В нижней части панели навигации выберите "Библиотека программного обеспечения" (слева в основном окне).
3. В верхней части панели навигации в окне структуры раскройте ветвь "Управление приложениями" (слева в основном окне).
4. Вызовите контекстное меню объекта "Приложения" и выберите команду "Создать приложение".

   На экране появится диалог, подобный следующему.

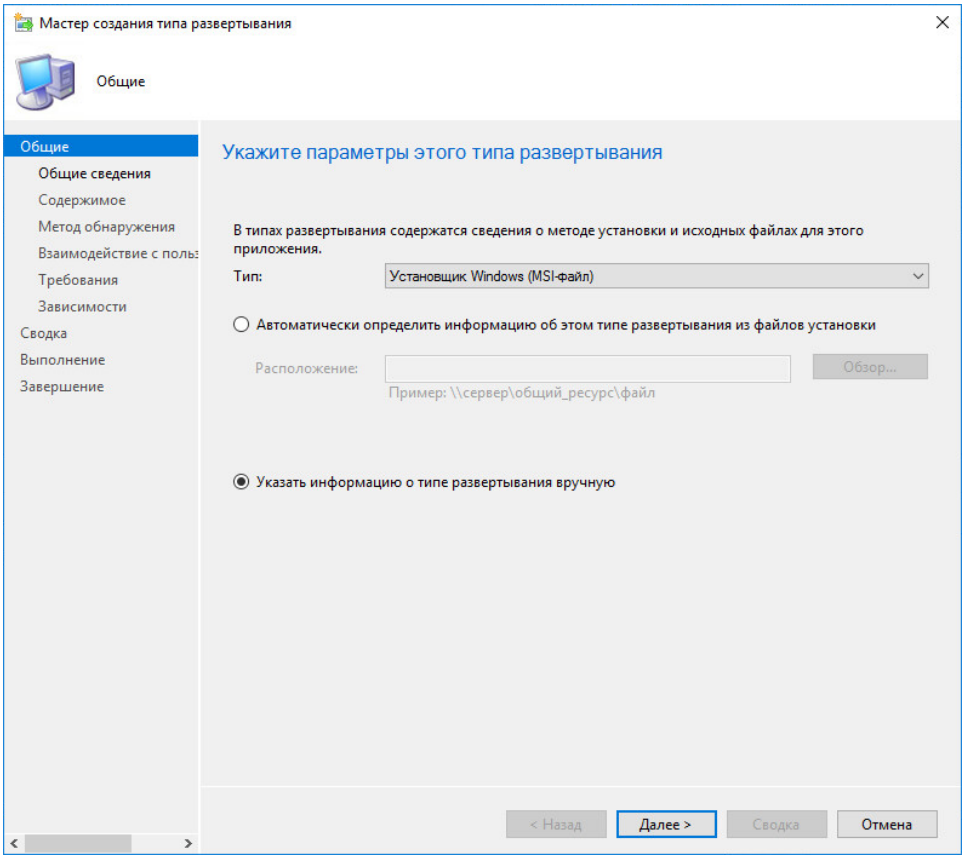


5. В диалоге установите отметку в поле "Вручную задать сведения о приложении" и нажмите кнопку "Далее >".

   На экране появится диалог, подобный следующему.

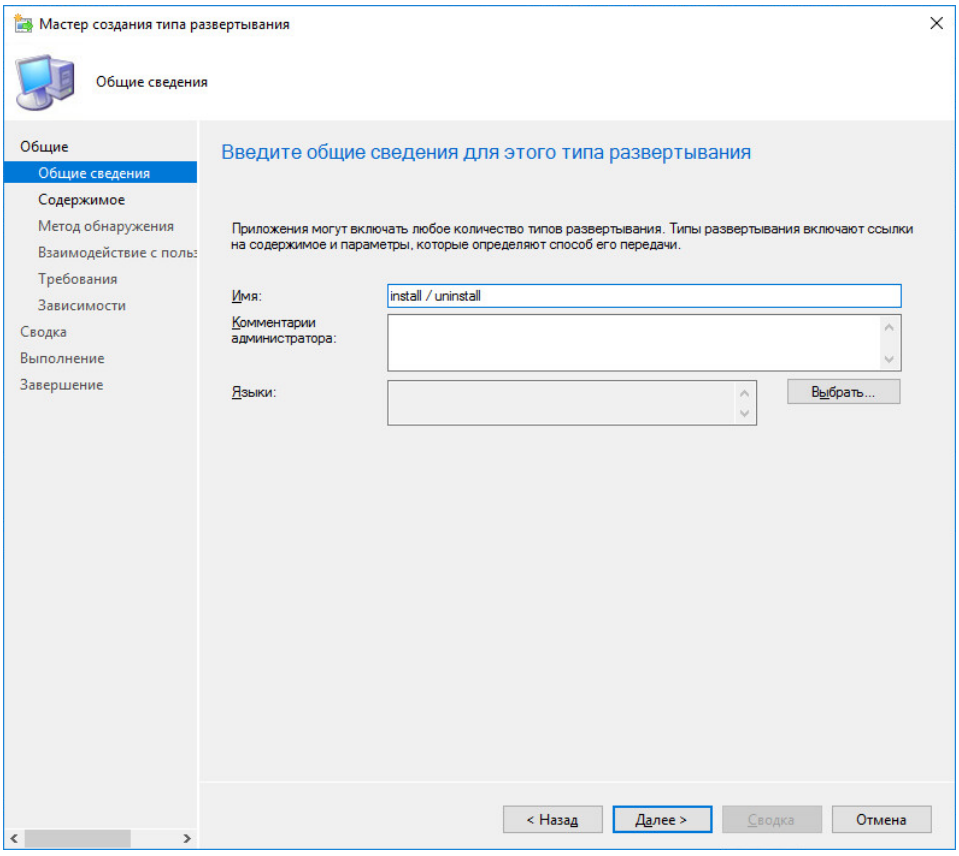


6. В поле "Имя" укажите название приложения и нажмите кнопку "Далее >".
   На экране появится диалог "Каталог приложений".
7. Нажмите кнопку "Далее >".
   На экране появится диалог "Типы развертывания".
8. Нажмите кнопку "Добавить".
   На экране появится диалог создания типа развертывания.



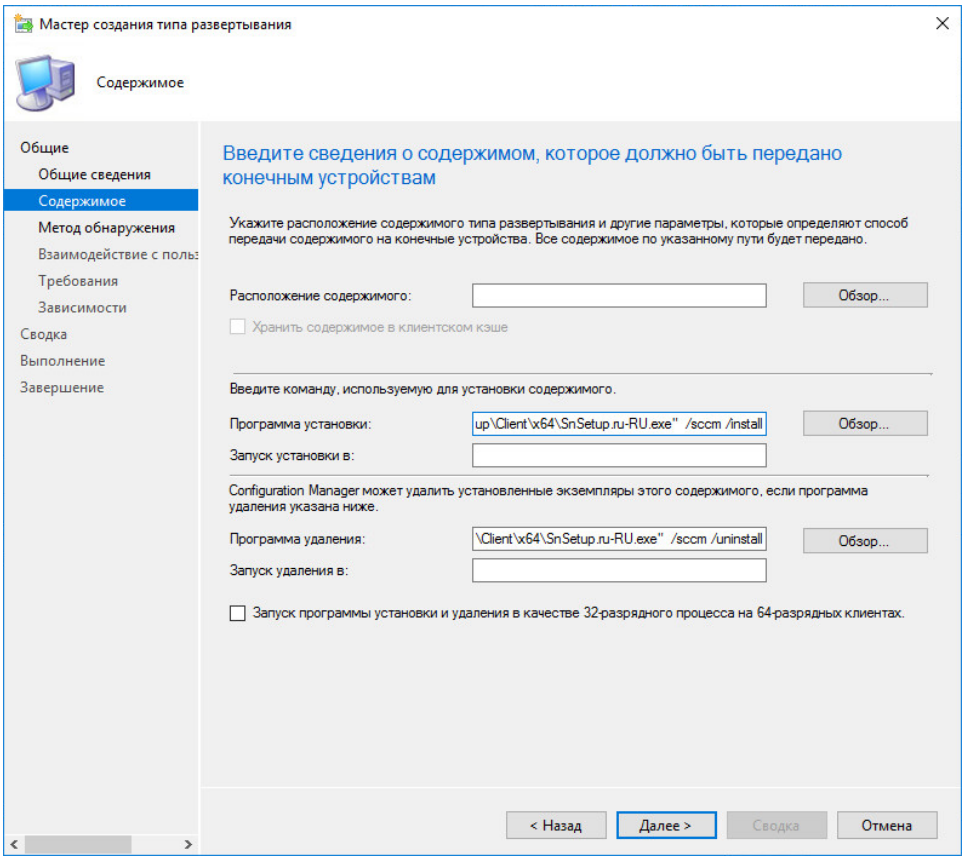
9. В поле "Тип" укажите "Установщик Windows (MSI-файл)", установите отметку в поле "Указать информацию о типе развертывания вручную" и нажмите кнопку "Далее >".

На экране появится диалог, подобный следующему.



10. В поле "Имя" укажите название типа развертывания и нажмите кнопку "Далее >".

На экране появится диалог "Содержимое".



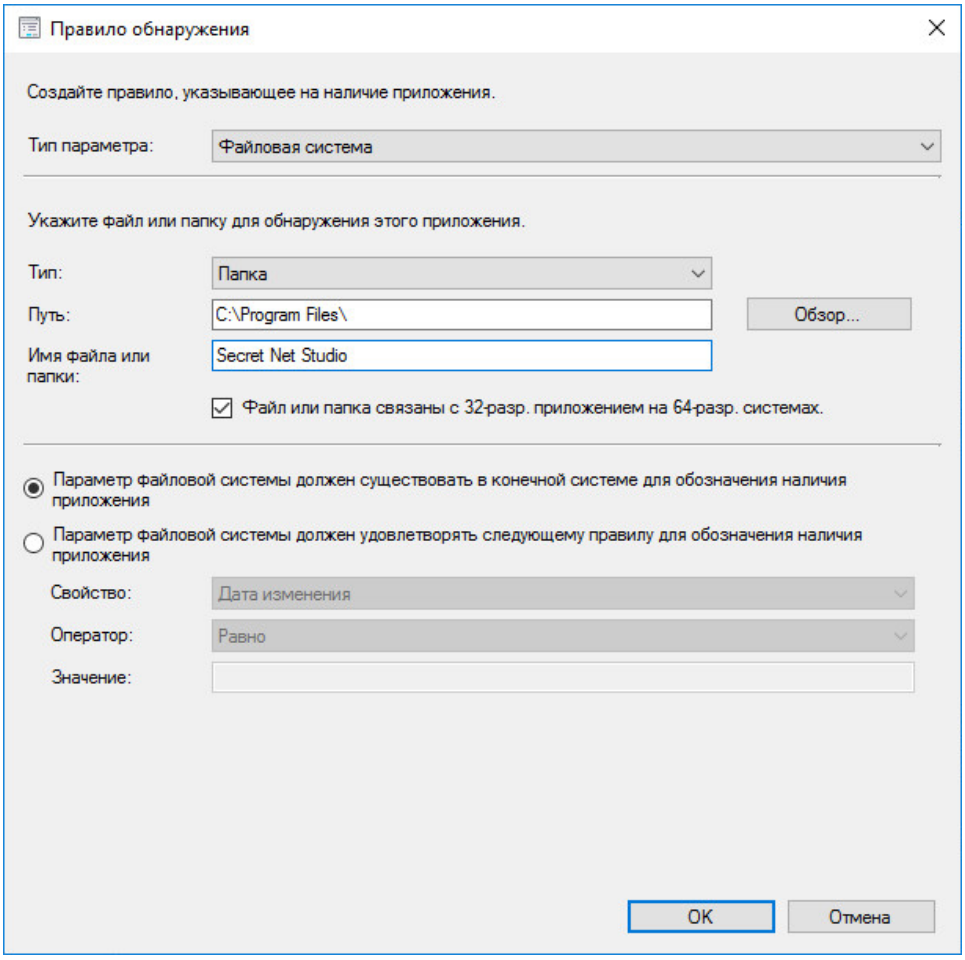
11. Для типа развертывания выполните следующие действия:

- Укажите информацию:
  - в поле "Программа установки" укажите в соответствующем формате путь к дистрибутиву и команду (см. стр.**85**);
  - в поле "Программа удаления" укажите в соответствующем формате путь к дистрибутиву и команду (см. стр.**85**).
- Нажмите кнопку "Далее >".

На экране появится диалог "Метод обнаружения".

12. Нажмите кнопку "Добавить".

На экране появится диалог создания правил обнаружения.



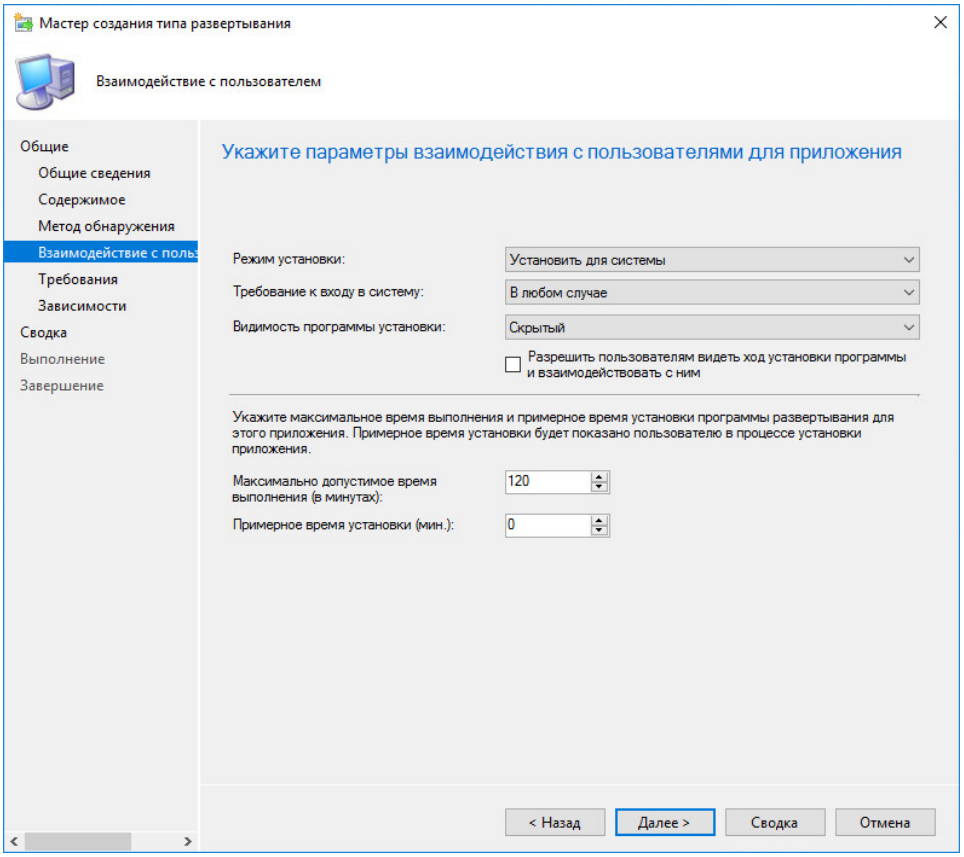
13. Для настройки правила обнаружения выполните следующие действия:

- Укажите следующее условие для правила обнаружения:
  - в поле "Путь" укажите путь к папке \Program Files;
  - в поле "Имя файла или папки" укажите имя папки \Secret Net Studio.
- Нажмите кнопку "OK".

В списке появится новое правило обнаружения.

14. Нажмите кнопку "Далее >".

На экране появится диалог "Взаимодействие с пользователями".



15. Для настройки взаимодействия с пользователями выполните следующие действия:
    - Укажите информацию:
        - в поле "Режим установки" укажите "Установить для системы";
        - в поле "Требование к входу в систему" укажите "В любом случае";
        - в поле "Видимость программы установки" укажите "Скрытый".
    - Нажмите кнопку "Далее >".

    На экране появится диалог требований.
16. Нажмите кнопку "Далее >".

    На экране появится диалог зависимости.
17. Нажмите кнопку "Далее >".

    На экране появится диалог подтверждения параметров развертывания.
18. В диалоге проверьте содержимое и нажмите кнопку "Далее >".

    Начнется процесс содания типа развертывания.
19. После завершения нажмите кнопку "Закрыть".

    На экране в диалоге "Типы развертывания" появится новый элемент.
20. Нажмите кнопку "Далее >".

    На экране появится диалог подтверждения параметров приложения.
21. В диалоге проверьте содержимое и нажмите кнопку "Далее >".

    Начнется процесс содания приложения.
22. После завершения нажмите кнопку "Закрыть".

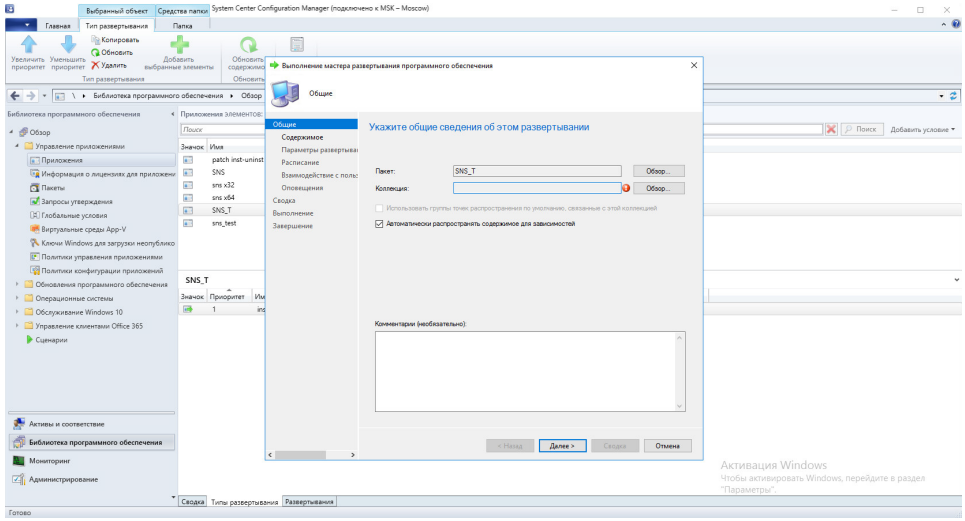
    По окончании процесса в списке появится новый элемент, содержащий сведения о созданном приложении.

Примечание. Для создания приложений по установке и удалению пакетов обновлений используется аналогичный алгоритм.

Для установки созданного приложения:

1. Откройте System Center Configuration Manager.
2. В нижней части панели навигации выберите "Библиотека программного обеспечения" (слева в основном окне).
3. В верхней части панели навигации в окне структуры раскройте ветвь "Управление приложениями" (слева в основном окне).
4. Выберите объект "Приложения".
5. В списке созданных приложений выберите созданное ранее приложение.
6. Вызовите контекстное меню приложения и выберите команду "Развернуть".

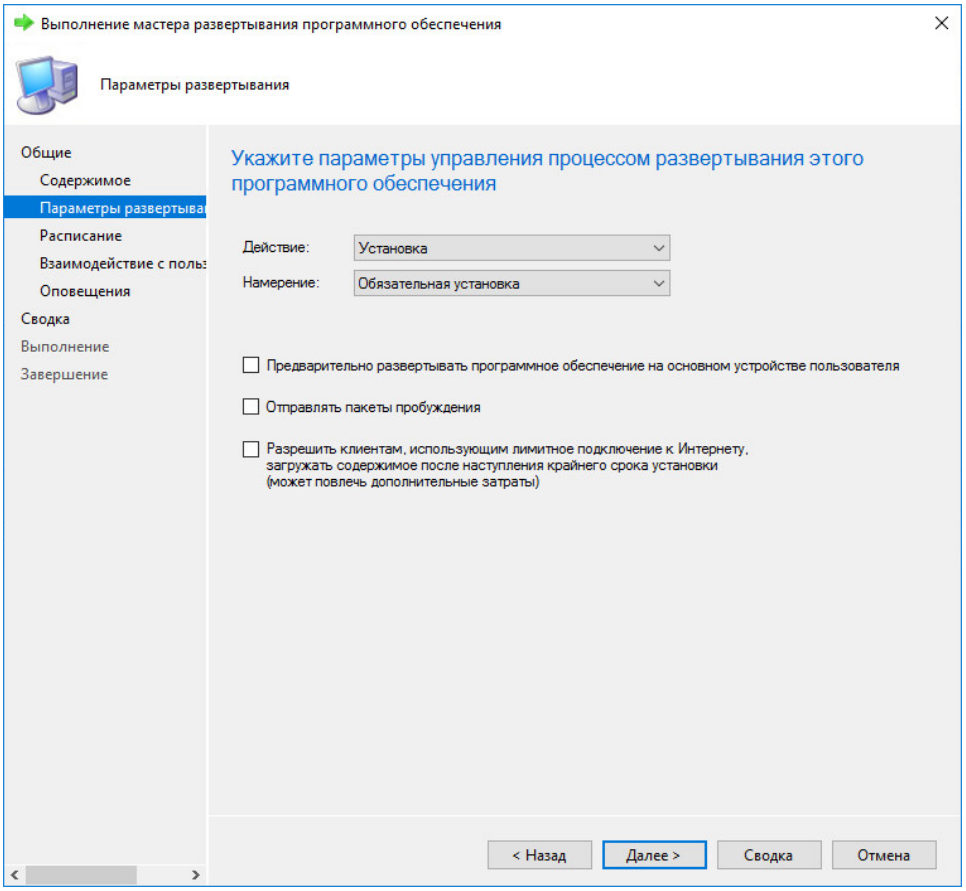
   На экране появится диалог, подобный следующему.



7. Напротив поля "Коллекция" нажмите кнопку "Обзор" и в появившемся списке выберите необходимую коллекцию компьютеров, на которую требуется установить пакет установки, а затем нажмите кнопку "ОК".
8. Нажмите кнопку "Далее >".

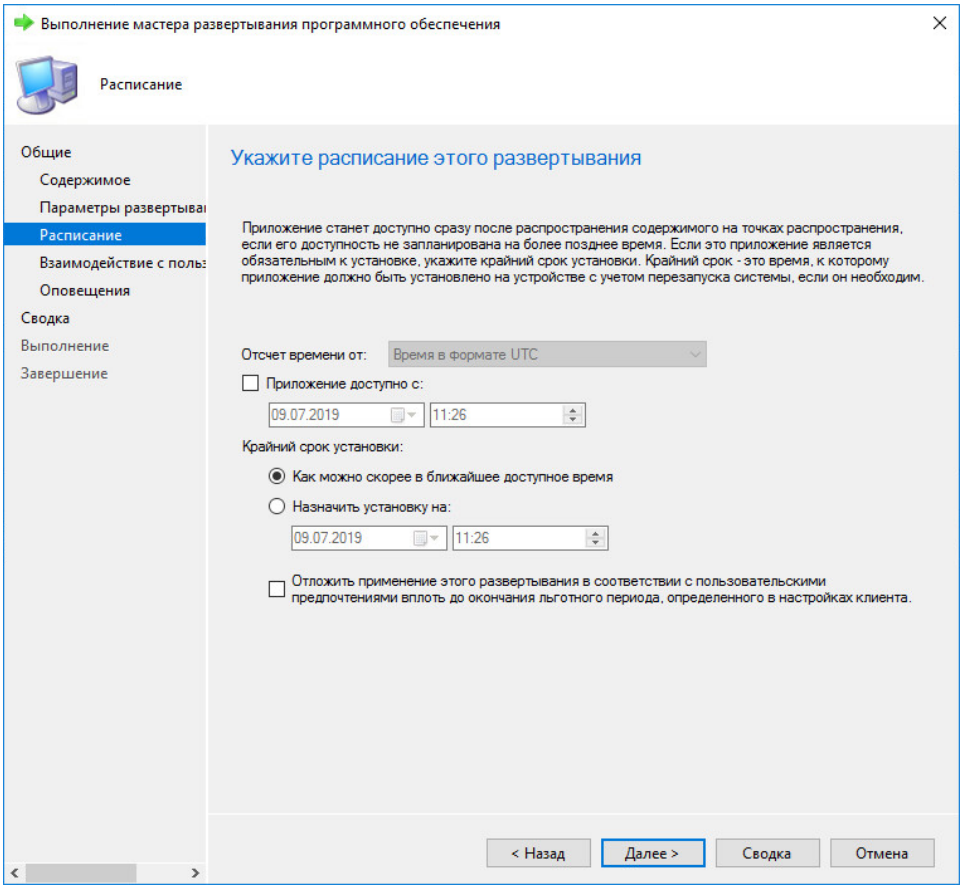
   На экране появится диалог места распространения содержимого.
9. Нажмите кнопку "Далее >".

   На экране появится диалог параметров управления процессом развертывания этого программного обеспечения.



10. В поле "Намерение" укажите "Обязательная установка" и нажмите кнопку "Далее >".

На экране появится диалог расписания развертывания этого программного обеспечения.



Примечание. Если требуется выполнить удаление, то в поле "Действие" укажите "Удаление", параметр "Обязательная установка" в поле "Намерение" будет установлен автоматически.

11. Нажмите кнопку "Далее >".

    На экране появится диалог параметров взаимодействия с пользователем при установке этого программного обеспечения.

12. Нажмите кнопку "Далее >".

    На экране появится диалог параметров оповещений.

13. Нажмите кнопку "Далее >".

    На экране появится диалог подтверждения параметров этого развертывания.

14. В диалоге проверьте содержимое и нажмите кнопку "Далее >".

    Начнется процесс установки приложения.

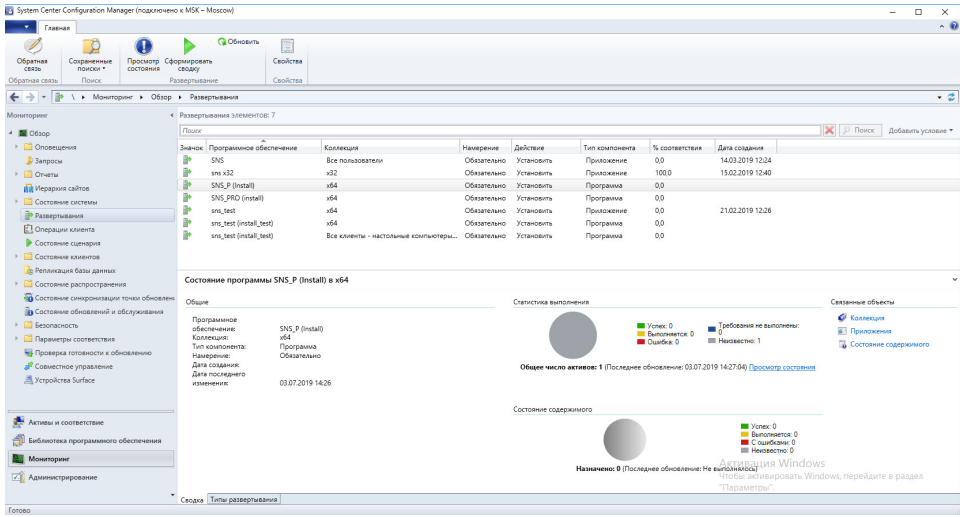
15. После завершения нажмите кнопку "Закрыть".

Примечание. Для команд обновления и исправления ПО приложение не используется.

Для отслеживания процесса выполнения приложения:

1. Откройте System Center Configuration Manager.
2. В нижней части панели навигации выберите "Мониторинг" (снизу в основном окне).
3. В верхней части панели навигации в окне структуры выберите "Развертывания".

   На экране появится диалог, подобный следующему.



4. В списке программного обеспечения выберите требуемое приложение и посмотрите его состояние.

Глава 8
Обновление и переустановка компонентов

Обновление

В системе Secret Net Studio реализована возможность обновления ПО предыдущих версий на текущую версию. При обновлении сохраняются заданные параметры настройки системы (для некоторых параметров могут быть выставлены значения по умолчанию, если сохранение прежних значений технически невозможно).

Обновление компонентов на компьютерах системы осуществляется по отдельности с помощью программ установки компонентов. При этом для клиента Secret Net Studio в сетевом режиме функционирования обновление может выполняться централизованно под управлением сервера безопасности.

Внимание!

- Для обновления Secret Net Studio с версии 8.5 на версию 8.7 необходимо предварительно установить на клиенты пакет обновлений 8_5_5329_169_Inc107095_Build112.
- При обновлении Secret Net Studio с версии 8.2 и более ранних, а также с любой версии Secret Net на Secret Net Studio версии 8.6 необходимо сначала выполнить обновление на Secret Net Studio версии 8.6 (сборка 8.6.8330.0) и затем выполнить установку пакетов исправлений. Данное требование актуально для тех случаев, когда в механизме контроля устройств Secret Net Studio используется политика, запрещающая подключение новых устройств для классов "Физические диски" и/или "Оптические диски" (см. главу "Настройка контроля устройств" документа [2]).

Порядок обновления компонентов централизованного управления

Обновление компонентов Secret Net Studio, реализующих централизованное управление, осуществляется в следующей последовательности:

1. Включите все контроллеры домена.
2. Обновите ПО серверов безопасности на текущую версию (см. стр.**99**). Если в домене безопасности имеется несколько серверов, процедуру обновления нужно начать с сервера, которому присвоена роль мастера схемы LDS домена безопасности. Обычно роль мастера схемы присвоена первому установленному серверу.
3. Обновите Центр управления (см. стр. **102**) на рабочих местах администраторов.
4. Обновите ПО клиента (см. стр.**102**) в следующем порядке:
   - серверы безопасности;
   - компьютеры сотрудников.

   Совет. При большом количестве компьютеров целесообразно применить автоматическое обновление клиента путем централизованной установки под управлением сервера безопасности (см. стр.**64**).
5. В Центре управления проверьте и при необходимости отредактируйте структуру оперативного управления (см. стр.**135**).

Обновление сервера безопасности

Обновление сервера безопасности выполняется пользователем, входящим в локальную группу администраторов компьютера.

Для выполнения некоторых действий при обновлении сервера безопасности могут потребоваться особые права доступа. Например, права на администрирование леса доменов безопасности и домена безопасности. Если пользователь, выполняющий установку, не обладает нужными правами, программа установки на определенных этапах может запрашивать учетные данные пользователей с правами доступа.

Внимание! При обновлении сервера безопасности процесс обновления нельзя прерывать и нужно довести до завершения. Если при замене модулей и модификации структур баз данных возникнут ошибки (например, по причинам недостаточных прав доступа или недоступности сервисов), будет выполнен возврат к предыдущему состоянию сервера (до обновления). Минимально необходимые условия для успешного обновления:

- работоспособное состояние сервера безопасности предыдущей версии;
- наличие прав администратора леса доменов безопасности — при первом обновлении в лесу доменов;
- наличие прав администратора домена безопасности.

В Secret Net Studio версий 8.0-8.5 и Secret Net версий 7.x при установке сервера безопасности на контроллерах домена AD программа установки создавала служебную учетную запись доменного пользователя SecretNetLDS$ или SecretNetLDS (в зависимости от версии ОС), используемую для запуска служб AD LDS. Эта учетная запись в текущей версии Secret Net Studio не требуется.

Внимание! После обновления ПО всех серверов безопасности до текущей версии данную учетную запись необходимо в обязательном порядке удалить. Перед выполнением удаления необходимо вначале обновить ПО сервера безопасности на всех без исключения контроллерах домена AD, на которых он функционирует. Затем на одном из контроллеров домена следует запустить на выполнение под учетной записью администратора домена AD утилиту lds_dc_patch.exe с параметром del — lds_dc_patch.exe /del. Утилита размещается на установочном диске Secret Net Studio в каталоге Tools\SecurityCode\LdsPasswordChange\.

Для обновления сервера безопасности:

1. Вставьте в привод установочный диск системы Secret Net Studio. Дождитесь появления окна программы автозапуска (см. стр.**48**) и запустите обновление с помощью команды "Сервер безопасности".

   Примечание. Запуск обновления можно выполнить вручную без использования программы автозапуска. Для этого запустите с установочного диска файл \Setup\Server\x64\setup.ru-RU.exe.

   После запуска программы установки выполняется анализ системы на соответствие программным и аппаратным требованиям для установки компонента. При этом проверяется текущее состояние встроенного в ОС механизма управления учетными записями (User Account Control — UAC).

   Внимание! Если механизм UAC включен — на экране появится диалог запроса на его временное отключение. В этом случае нажмите кнопку "Да" для отключения механизма, перезагрузите компьютер и только после этого снова запустите процедуру обновления сервера безопасности.

   По окончании проверки системы на экран будет выведен диалог с сообщением о готовности к началу обновления и позволяющий также дополнительно выбрать для установки службу синхронизации.

   Пояснение. Служба синхронизации устанавливается на сервере безопасности, чтобы, выполняя функцию шлюза, обеспечить взаимодействие этого сервера с родительским сервером безопасности. Установка данной службы выполняется отдельной программой установки, которая будет автоматически запущена после завершения обновления сервера безопасности (см. стр.**58**).

2. Нажмите кнопку "Обновить" или отметьте поле "Служба синхронизации" и нажмите кнопку "Изменить".

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.

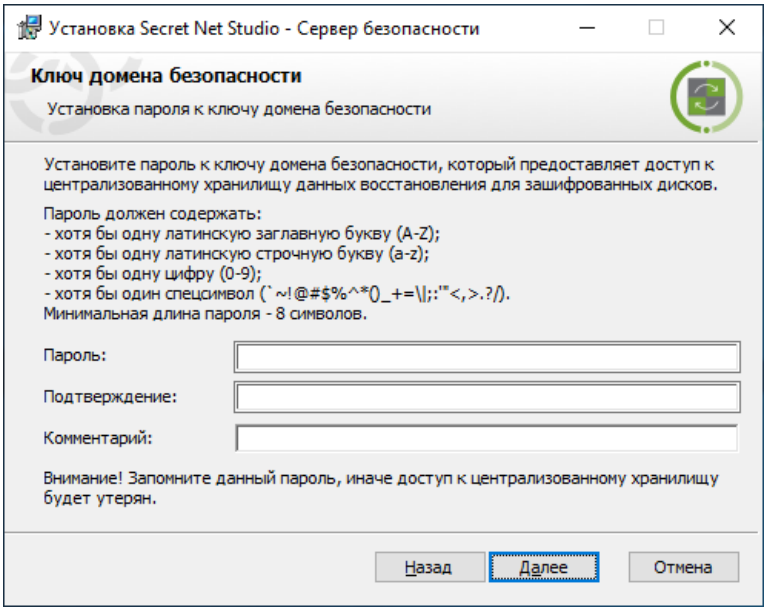
Примечание. Перед выполнением дальнейших действий рекомендуется закрыть программу автозапуска.

3. Нажмите кнопку "Далее".

   На экране появится диалог принятия лицензионного соглашения.

4. Ознакомьтесь с содержанием лицензионного соглашения, отметьте пункт о его принятии и нажмите кнопку "Далее".

   На экране появится диалог "Ключ домена безопасности".



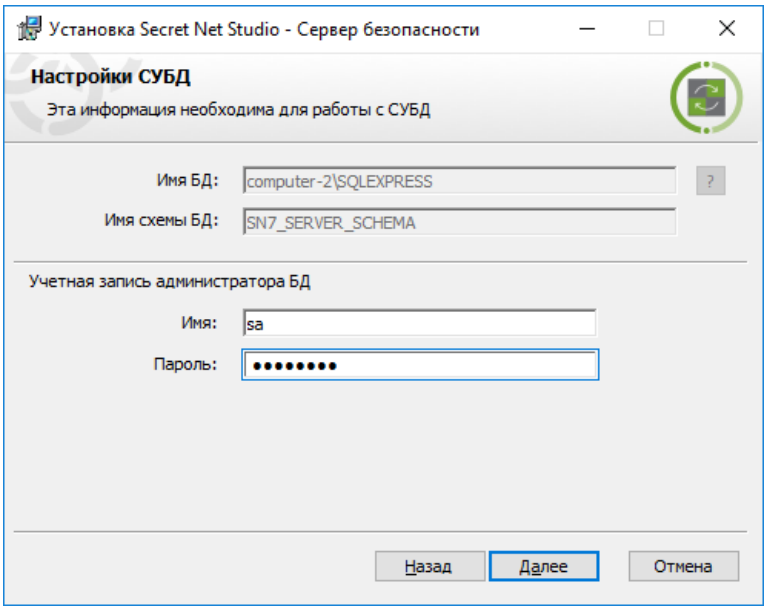
5. Установите пароль к ключу домена безопасности. Ключ и пароль предназначены для предоставления доступа к централизованному хранилищу данных восстановления для зашифрованных дисков.

Внимание!

- Пароль должен удовлетворять требованиям, указанным в диалоге.
- Запомните пароль к ключу домена безопасности, иначе доступ к централизованному хранилищу данных восстановления будет утерян.

Введите подтверждение пароля. При необходимости укажите комментарий к паролю.Нажмите кнопку "Далее".

На экране появится диалог "Настройки СУБД". Пример содержимого диалога представлен на следующем рисунке.



6. В группе полей "Учетная запись администратора БД" укажите учетные данные администратора базы данных на СУБД и нажмите кнопку "Далее".

   На экране появится диалог "Все готово к обновлению".

7. Нажмите кнопку "Обновить".

   Начнется процесс обновления программных модулей.

   Внимание! Если некоторые программные модули в данный момент используются, на экране появится диалог запроса на обновление файлов или служб, которые невозможно обновить. В этом случае нажмите кнопку "ОК" для начала процесса обновления.

   Если при выполнении действия **2** была выбрана установка службы синхронизации, будет запущена программа установки этой службы. Выполните ее установку так, как это описано на стр.**58**

   После завершения всех операций появится сообщение с предложением перезагрузить компьютер.

8. Перезагрузите компьютер и дождитесь загрузки системы.

   Пояснение. Информация о сервере безопасности в структуре оперативного управления может обновиться с некоторой задержкой. В Центре управления, подключенной к другому серверу безопасности, загрузка обновленной структуры с новыми данными может произойти через несколько минут после обновления ПО СБ (порядка 10–15 минут).

Обновление Центра управления

Обновление Центра управления выполняется пользователем, входящим в локальную группу администраторов компьютера. Для запуска процедуры обновления компонента используйте установочный диск (см. стр.**59**). Процедура обновления выполняется без особенностей.

Обновление клиента

Обновление клиента выполняет пользователь, входящий в локальную группу администраторов компьютера.

Для выполнения некоторых действий при обновлении клиента могут потребоваться особые права доступа. Например, права на администрирование домена безопасности, если клиент подчинен серверу безопасности. Если пользователь, выполняющий установку, не обладает нужными правами, программа установки на определенных этапах может запрашивать учетные данные пользователей с правами доступа.

Примечание. Secret Net Studio версии 8.7 не поддерживает одновременную работу механизма защиты дисков и доверенной среды, а также механизма полнодискового шифрования и доверенной среды. Если на компьютере используется версия клиента, где одновременно работают оба компонента, то обновление будет невозможно. Перед обновлением необходимо отключить один из компонентов.

Для обновления клиента:

1. Вставьте в привод установочный диск системы Secret Net Studio. Дождитесь появления окна программы автозапуска (см. стр.**48**) и запустите обновление с помощью команды "Защитные компоненты".

   Примечание. Запуск обновления можно выполнить вручную без использования программы автозапуска. Для этого в зависимости от операционной системы компьютера выполните следующее действие:
   - при установке на компьютер с 64-разрядной версией Windows — запустите с установочного диска файл \Setup\Client\x64\SnSetup.ru-RU.exe;
   - при установке на компьютер с 32-разрядной версией Windows — запустите с установочного диска файл \Setup\Client\Win32\SnSetup.ru-RU.exe.

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.

Примечание. Перед выполнением дальнейших действий рекомендуется закрыть программу автозапуска.

2. Нажмите ссылку "Пакеты исправлений..." для просмотра и выбора пакетов исправлений, которые будут применены при обновлении ПО.

Примечание. Пакеты исправлений можно установить отдельно от обновления системы защиты. Для этого запустите требуемый файл пакета исправлений на установочном диске в папке Tools\SecurityCode\Patches\.

3. Нажмите кнопку "Готово".

   На экране появится окно запроса с предложением перезагрузить компьютер.

4. Нажмите кнопку "Да" в окне запроса.

   Начнется перезагрузка компьютера, во время которой выполняется обновление компонентов Secret Net Studio. После успешного входа пользователя в систему над пиктограммой Secret Net Studio, находящейся на панели задач Windows, появится сообщение об успешном завершении обновления.

Особенности установки клиента в режиме обновления других продуктов

При установке клиента Secret Net Studio проверяется наличие установленного ПО следующих продуктов компании "Код Безопасности":

- СЗИ Secret Net (клиентское ПО);
- СЗИ Security Studio Endpoint Protection;
- СЗИ TrustAccess.

Функциональные возможности перечисленных продуктов могут быть реализованы частично или полностью механизмами защиты клиента Secret Net Studio.

Если обнаружен какой-либо из указанных продуктов, в зависимости от ситуации возможны следующие варианты:

- обновление (замена) имеющейся версии продукта с применением ранее заданных параметров в соответствующих подсистемах клиента Secret Net Studio, если для этого имеется техническая возможность;
- установка клиента Secret Net Studio с сохранением имеющейся версии продукта для самостоятельного функционирования (без интеграции);
- отмена установки клиента.

Установка при наличии СЗИ Secret Net (клиентское ПО)

При наличии клиентского ПО СЗИ Secret Net выполняется обновление этого ПО на устанавливаемую версию клиента Secret Net Studio. После обновления будут действовать защитные подсистемы клиента Secret Net Studio, которые были указаны для установки.

Установка при наличии СЗИ TrustAccess

При наличии ПО СЗИ TrustAccess возможны следующие варианты:

- для версий 1.3.x — выполняется обновление, если в списке устанавливаемых защитных подсистем указан хотя бы один из компонентов сетевой защиты. В противном случае сохраняется имеющаяся версия продукта;
- для остальных версий — в процессе установки выводится сообщение об ошибке из-за неподдерживаемой версии продукта. В этом случае необходимо вручную выполнить процедуру удаления ПО.

Переустановка (восстановление)

Для восстановления нарушенной работоспособности компонентов системы Secret Net Studio может применяться процедура переустановки ПО. Переустановка выполняется с использованием дистрибутива той же версии, которая установлена на компьютере.

Переустановку должен выполнять пользователь, входящий в локальную группу администраторов компьютера.

Примечание. В текущей реализации не предусмотрена процедура переустановки ПО сервера безопасности.

Переустановка клиента

Запуск процедуры переустановки клиента можно выполнить так же, как и запуск установки в интерактивном режиме (см. стр.60), или использовать стандартный способ переустановки для компонента "Secret Net Studio – С" в окне ОС Windows "Программы и компоненты". После запуска программы установки на экран будет выведен диалог для выбора варианта действий.

Для переустановки клиента с восстановлением ПО:

1. В диалоге выбора варианта действий установите отметку в поле "исправить" и нажмите кнопку "Готово".

   На экране появится окно запроса с предложением перезагрузить компьютер.

2. Нажмите кнопку "Да" в окне запроса.

   Начнется перезагрузка компьютера, во время которой будет выполнена повторная установка компонентов Secret Net Studio. После успешного входа пользователя в систему над пиктограммой Secret Net Studio, находящейся на панели задач Windows, появится сообщение об успешном завершении данной процедуры.

Переустановка Центра управления

При переустановке Центра управления выполняется его восстановление.

Запуск процедуры переустановки осуществляется так же, как и запуск установки (см. стр.59). После диалога приветствия на экран будет выведен диалог для выбора варианта действий.

Для переустановки Центра управления:

1. В диалоге для выбора варианта действий нажмите кнопку "Восстановить".

   На экране появится диалог, сообщающий о готовности к установке.

2. Нажмите кнопку "Восстановить".

   Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса. При их завершении на экране появится диалог "Установка завершена".

3. Нажмите кнопку "Готово", а затем нажмите кнопку "Закрыть" в еще одном появившемся на экране диалоге.

Глава 9
Удаление компонентов

Предупреждение.
- Если на защищаемых компьютерах имеется конфиденциальная или зашифрованная информация, следует принять меры для ее защиты и сохранения до удаления системы Secret Net Studio.
- При наличии на компьютере дисков, зашифрованных с помощью механизма полнодискового шифрования, невозможно удалить клиент Secret Net Studio.

Порядок удаления в сетевом режиме функционирования

Удаление клиентов Secret Net Studio в сетевом режиме функционирования и компонентов для централизованного управления рекомендуется выполнять в следующем порядке:

1. Удалите ПО клиентов на всех компьютерах.
2. Удалите Центр управления на рабочих местах администраторов.
3. Удалите ПО серверов безопасности.

Удаление клиента

ПО клиента можно удалить при работе на компьютере локально или в терминальной сессии. Для сетевого режима функционирования также предусмотрен метод централизованного удаления под управлением сервера безопасности. Централизованное удаление реализуется с помощью Центра управления (см. стр. **64**). Для этого необходимо сформировать задания на удаление ПО, аналогичные заданиям развертывания.

Ниже рассматривается процедура локального удаления клиента.

Процедуру удаления должен выполнять пользователь, входящий в локальную группу администраторов компьютера.

Для удаления клиента:

1. Выполните запуск процедуры установки клиента в интерактивном режиме (см. стр. **60**) или используйте стандартный способ запуска удаления для компонента "Secret Net Studio" в окне ОС Windows "Программы и компоненты".

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог для выбора варианта продолжения.
2. В диалоге установите отметку в поле "удалить" и укажите учетные данные пользователя с правами администратора домена безопасности.

   Пояснение. Если текущий пользователь имеет права на запись в хранилище объектов централизованного управления — оставьте отмеченным поле "использовать для подключения учетную запись текущего пользователя". Если права не предоставлены — выберите пункт "использовать указанные ниже имя и пароль" и введите данные соответствующей учетной записи.
3. Нажмите кнопку "Готово".

   Если на компьютере включена функция "Контроль административных привилегий", на экране появится диалоговое окно ввода PIN администратора. Для продолжения процедуры удаления введите PIN и нажмите кнопку "ОК".

   Начнется процесс удаления защитных подсистем.
4. После завершения всех операций удаления нажмите кнопку "Далее".

На экране появится завершающий диалог со сведениями о выполненных операциях и предложением перезагрузить компьютер.

Совет. При необходимости используйте ссылки в разделе "Информация" для выполнения следующих действий:

- чтобы посмотреть записи журнала трассировки — выберите ссылку "отчет об установке";
- чтобы собрать все необходимые для диагностики Secret Net Studio – C файлы и данные, в случае возникновения проблем при установке — выберите ссылку "диагностическую информацию".

5. Перезагрузите компьютер.

Удаление Центра управления

Процедура удаления Центра управления выполняется без особенностей. Запуск удаления компонента "Secret Net Studio — Центр управления" можно выполнить стандартным способом в окне ОС Windows "Программы и компоненты".

Удаление сервера безопасности

При удалении сервера безопасности следует иметь в виду, что все компьютеры, подчиненные данному серверу, станут свободными — то есть не подчиненными какому-либо серверу безопасности.

Для выполнения некоторых действий при удалении сервера безопасности могут потребоваться особые права доступа. Например, права, предоставленные группе администраторов домена безопасности. Если пользователь, выполняющий удаление, не обладает нужными правами, программа установки на определенных этапах может запрашивать учетные данные пользователей с правами доступа.

Для удаления сервера безопасности:

1. В окне ОС Windows "Программы и компоненты" выберите в списке компонент "Secret Net Studio — Сервер безопасности" и нажмите кнопку "Удалить".

   На экране появится диалог запроса на удаление компонента.

2. Нажмите кнопку "Да" в диалоге запроса.

   Программа установки проверит текущее состояние встроенного в ОС механизма управления учетными записями (User Account Control — UAC). Возможны следующие варианты:

   - если механизм UAC включен — на экране появится диалог запроса на его временное отключение. В этом случае нажмите кнопку "Да" для отключения механизма, перезагрузите компьютер и после этого снова запустите процедуру удаления сервера безопасности (см. действие **1**);
   - если механизм UAC отключен — процедура удаления будет продолжена, и на экране появится диалог программы установки, содержащий сведения о ходе выполнения операций. На этапе выбора действий с базой данных сервера на экране появится диалог "Удаление базы данных".

3. Выполните нужное действие:

   - для сохранения БД — нажмите кнопку "Отмена";
   - для удаления БД — введите учетные данные администратора базы данных на сервере СУБД в полях "Имя администратора" и "Пароль администратора" и нажмите кнопку "ОК".

   Процедура удаления будет продолжена. На этапе выбора действий с сертификатом сервера на экране появится запрос об удалении сертификата.

4. Чтобы удалить сертификат сервера безопасности из IIS, нажмите кнопку "Да" в диалоге запроса. При необходимости сохранить сертификат в IIS нажмите кнопку "Нет".

   После завершения всех операций удаления в диалоге программы установки появится предупреждение о необходимости перезагрузки компьютера.

5. Перезагрузите компьютер.

Удаление шлюза

Если на сервере безопасности установлено и используется ПО шлюза, его можно удалить отдельно от сервера, предварительно удалив шлюз из структуры ОУ.

Внимание! При удалении настроенного и функционирующего шлюза необходимо учитывать, что взаимодействие между родительским и дочерним лесами безопасности будет прекращено. В результате управление защищаемыми компьютерами дочернего леса средствами корневого сервера безопасности станет невозможно.

Рекомендуется выполнять данную операцию в указанном ниже порядке.

Для удаления шлюза:

Шаг 1. Удалите шлюз из структуры ОУ:

1. Запустите Центр управления и подключитесь к родительскому серверу безопасности, на котором зарегистрирован шлюз.
2. В Центре управления в нижней части панели навигации нажмите кнопку "Настройки" и в появившейся панели нажмите ссылку "Конфигурирование".

   На экране появится диалог выбора режима работы.
3. Выберите вариант "Редактирование иерархии лесов безопасности".

   На экране появится диалог редактирования списка шлюзов.
4. Выберите нужный шлюз, нажмите кнопку "Удалить" и подтвердите свое решение в появившемся окне запроса.

   Начнется процесс удаления шлюза, занимающий некоторое время. Информация о ходе этого процесса отображается в виде сообщений в панели событий системы. Дождитесь его завершения и удаления из списка выбранного шлюза. После этого из иерархической структуры ОУ также будет удален соответствующий данному шлюзу лес безопасности.
5. Нажмите кнопку "Закрыть".

Шаг 2. Удалите ПО шлюза:

1. На компьютере, на котором установлено ПО шлюза, запустите программу установки сервера безопасности той же версии, что и установленный здесь сервер.

   Программа установки проверит текущее состояние встроенного в ОС механизма управления учетными записями (User Account Control — UAC). Возможны следующие варианты:
   - если механизм UAC включен — на экране появится диалог запроса на его временное отключение. В этом случае нажмите кнопку "Да" для отключения механизма, перезагрузите компьютер и после этого снова запустите программу установки сервера безопасности;
   - если механизм UAC отключен — процедура будет продолжена, и на экране появится диалог программы установки, содержащий сведения об установленных компонентах.
2. Удалите отметку из поля "Служба синхронизации" и нажмите кнопку "Изменить".

   Начнется процесс удаления службы синхронизации, по окончании которого в информационном окне появится сообщение об этом.
3. Нажмите кнопку "Закрыть".

Удаление отдельных подсистем клиента

Если на компьютере не используются некоторые из установленных защитных подсистем клиента Secret Net Studio, эти подсистемы можно удалить локально или в терминальной сессии. С учетом особенностей модульных взаимосвязей функциональных компонентов клиента, удаление может выполняться для следующих отдельных подсистем и групп:

- доверенная среда;
- паспорт ПО;
- подсистемы группы сетевой защиты;
- подсистемы защиты информации на локальных дисках и шифрования данных в криптоконтейнерах;
- подсистема контроля печати;
- подсистемы группы локальной защиты (кроме вышеуказанных подсистем).

Кроме того, предусмотрена возможность удаления Центра управления, установленного для работы в локальном режиме (при установке клиента).

Процедура удаления подсистем клиента должна выполняться пользователем, входящим в локальную группу администраторов компьютера.

Для удаления отдельных подсистем клиента:

1. Выполните запуск процедуры установки клиента в интерактивном режиме (см. стр. **60**) или используйте стандартный способ запуска удаления для компонента "Secret Net Studio" в окне ОС Windows "Программы и компоненты".

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог для выбора варианта продолжения.
2. В диалоге установите отметку в поле "удалить компоненты" и нажмите кнопку "Далее".

   Если на компьютере включена функция "Контроль административных привилегий", на экране появится диалоговое окно ввода PIN администратора.
3. Для продолжения процедуры удаления введите PIN и нажмите кнопку "ОК".

   На экране появится диалог для выбора удаляемых подсистем.
4. Отметьте элементы, которые нужно удалить, и нажмите кнопку "Готово".

   Начнется процесс удаления защитных подсистем.
5. После завершения всех операций удаления нажмите кнопку "Далее".

   На экране появится завершающий диалог со сведениями о выполненных операциях и предложением перезагрузить компьютер.

   Совет. При необходимости используйте ссылки в разделе "Информация" для выполнения следующих действий:
   - чтобы посмотреть записи журнала трассировки — выберите ссылку "отчет об установке";
   - чтобы собрать все необходимые для диагностики Secret Net Studio – C файлы и данные, в случае возникновения проблем при установке — выберите ссылку "диагностическую информацию".
6. Перезагрузите компьютер.

Удаление пакетов обновлений

Запуск процедуры удаления пакетов обновлений клиента можно выполнить так же, как и запуск установки в интерактивном режиме (см. стр. **60**), или использовать стандартный способ удаления для компонента "Secret Net Studio – C" в окне ОС Windows "Программы и компоненты". После запуска программы установки на экран будет выведен диалог для выбора варианта действий.

Для удаления пакетов обновлений:

1. В диалоге выбора варианта действий установите отметку в поле "удалить пакеты исправлений" и нажмите кнопку "Далее".

   Если на компьютере включена функция "Контроль административных привилегий", на экране появится диалоговое окно ввода PIN администратора. Для продолжения процедуры удаления введите PIN и нажмите кнопку "OK".

   На экране появится диалог выбора пакетов обновлений для удаления.

2. Выберите пакеты обновлений, которые необходимо удалить. Для выбора всех пакетов обновлений нажмите кнопку "Выбрать все". Нажмите кнопку "Готово".

   На экране появится окно запроса с предложением перезагрузить компьютер.

3. Нажмите кнопку "Да" в окне запроса.

   Начнется перезагрузка компьютера, во время которой будет выполнено удаление выбранных пакетов обновлений Secret Net Studio. После успешного входа пользователя в систему над пиктограммой Secret Net Studio, находящейся на панели задач Windows, появится сообщение об успешном завершении данной процедуры.

Глава 11
Управление Secret Net Studio

Организация управления системой защиты

Централизованное и локальное управление

Локальное управление — это управление работой механизмов защиты отдельного компьютера, которое осуществляется администратором безопасности непосредственно на компьютере. Локальное управление используется в тех случаях, когда возможности централизованного управления для отдельного компьютера недоступны или нецелесообразны. Например, если требуется обеспечить безопасную работу локальных пользователей компьютера. Программные средства локального управления установлены по умолчанию и могут использоваться пользователями, входящими в локальную группу администраторов компьютера.

Централизованное управление параметрами Secret Net Studio осуществляется администратором безопасности со своего рабочего места. Для этих целей может использоваться любой компьютер сети с установленными средствами централизованного управления.

В автономном режиме функционирования клиента Secret Net Studio доступны только возможности локального управления. В сетевом режиме управление можно осуществлять как локально, так и централизованно.

Внимание! В соответствии с концепцией Secret Net Studio управление работой защищаемых компьютеров с установленным клиентом в сетевом режиме функционирования рекомендуется осуществлять централизованно. Централизованное управление имеет приоритет перед локальным управлением. Например, если в групповой политике некоторые параметры заданы централизованно, то локально на компьютере их изменить нельзя. Также в случае отключения защитных подсистем локальным администратором в Локальном центре управления, в журнале Secret Net Studio регистрируется событие тревоги.

Использование групповых политик

Для централизованной настройки и применения параметров безопасности на защищаемых компьютерах с установленным клиентом в сетевом режиме функционирования могут использоваться групповые политики. По умолчанию параметры заданы только в локальной политике, имеющей наименьший приоритет.

В дополнение к параметрам локальной политики могут быть заданы параметры в политиках доменов, организационных подразделений и серверов безопасности. Эти параметры применяются на компьютерах, которые относятся к соответствующим доменам, организационным подразделениям или серверам безопасности, независимо от заданных значений в локальной политике каждого компьютера.

Параметры групповых политик применяются в следующей последовательности:

- локальная политика;
- политика домена;
- политика организационного подразделения — применяется на всех компьютерах, входящих в это организационное подразделение;
- политика, заданная для сервера безопасности — применяется на всех компьютерах, подчиненных этому серверу безопасности.

При наличии иерархии серверов безопасности параметры политик этих серверов применяются последовательно — начиная с сервера, которому компьютеры подчинены непосредственно, и далее до корневого сервера в иерархии. Таким образом, параметры, заданные в политике корневого сервера безопасности, имеют наивысший приоритет.

Настройка параметров групповых политик осуществляется в Центре управления Secret Net Studio.

За счет использования разных групповых политик реализуется централизованное управление параметрами с учетом особенностей информационной системы. Например, можно настроить общие параметры для всех компьютеров в политике домена и дополнительно указать значения отдельных параметров в политиках организационных подразделений. Это позволит применять на компьютерах различных организационных подразделений единые общие параметры и при этом задать специфические значения для компьютеров отдельных подразделений.

Обновление групповых политик

Параметры групповых политик на защищаемых компьютерах обновляются автоматически, в соответствии с действием механизма применения политик ОС Windows. При необходимости администратор может использовать средства принудительного обновления политик, чтобы ускорить процесс применения централизованно заданных параметров на компьютерах.

Принудительное обновление групповых политик можно осуществлять с помощью следующих средств:

- команда применения групповых политик в Центре управления;
- стандартные инструменты командной строки gpudate и secedit.

После обновления политик может потребоваться перезагрузка компьютера или завершение текущего сеанса работы пользователя — чтобы применить параметры, которые действуют только при загрузке ОС или при входе пользователя в систему. Для этого предусмотрены специальные возможности как в Центре управления (команды для перезагрузки или выключения компьютеров), так и в указанных инструментах командной строки.

Делегирование административных полномочий

Делегирование позволяет передать некоторые функции по настройке и управлению пользователям, не входящим в доменную группу администраторов.

По умолчанию администраторы безопасности обладают всеми необходимыми полномочиями для настройки параметров механизмов защиты Secret Net Studio. Однако некоторые функции управления объектами, доступные администраторам домена, также могут потребоваться и администраторам безопасности для выполнения своих служебных обязанностей. В частности, административная смена паролей пользователей, создание и удаление пользователей и групп пользователей, а также настройка основных параметров учетных записей. Чтобы предоставить администраторам безопасности эти возможности, администратор домена может делегировать соответствующие задачи с помощью стандартных средств ОС Windows.

Процедура делегирования выполняется в оснастке "Active Directory — пользователи и компьютеры" с использованием специального мастера делегирования управления. Запуск мастера нужно выполнить для соответствующего контейнера AD — всего домена или отдельного организационного подразделения (в зависимости от того, какими объектами разрешено управлять администратору безопасности). В мастере делегирования укажите учетную запись администратора безопасности или группы и затем в списке задач установите отметки для следующих элементов:

- "Создание, удаление и управление учетными записями пользователей" (Create, delete, and manage user accounts);

- "Переустановить пароли пользователей и установить изменение пароля при следующей перезагрузке" (Reset user passwords and force password change at next logon);
- "Создание, удаление и управление группами" (Create, delete, and manage groups) — задача делегируется для организационных подразделений;
- "Изменение членства в группах" (Modify the membership of a group).

Обзор средств управления

Управление системой Secret Net Studio осуществляется с помощью специальных программных средств, устанавливаемых при развертывании системы. Средства управления предоставляют возможности для настройки системы и изменения состояния объектов, а также для контроля функционирования защищаемых компьютеров. В зависимости от назначения средства управления могут представлять собой отдельные программы или программные элементы, встраиваемые в другие средства в качестве дополнительных расширений.

Средства только для локального управления

Средства локального управления используются при работе пользователей и администраторов на защищаемом компьютере. Эти средства предназначены для выполнения действий, доступных только при локальном управлении (например, настройка параметров доступа к локальным ресурсам), для просмотра централизованно заданных параметров и для настройки тех параметров, которые не были заданы централизованно.

В состав средств, используемых только для локального управления, входят следующие программные средства:

- пиктограмма Secret Net Studio в Панели задач Windows;
- диалог "Secret Net Studio" в окне настройки свойств ресурса;
- "Программа настройки подсистемы полномочного управления доступом";
- "Управление Secret Net Studio" в Панели управления Windows.

Также при локальном администрировании могут использоваться следующие средства для централизованного и локального управления:

- "Локальный центр управления" (устанавливается в составе клиента Secret Net Studio);
- "Управление пользователями" (программа для настройки параметров локальных пользователей);
- "Контроль программ и данных".

Примечание. В данном разделе перечислены регулярно используемые средства управления. Для выполнения частных специфических задач могут использоваться дополнительные программные средства, описание работы с которыми приводится отдельно.

Пиктограмма Secret Net Studio

После установки клиентского ПО в системной области панели задач Windows появляется пиктограмма Secret Net Studio. Пиктограмма предназначена для оповещения пользователя о наличии действующей защиты, для запуска основных пользовательских команд управления и получения сведений. Запуск команд осуществляется из контекстного меню пиктограммы. Перечень предусмотренных команд представлен в таблице.

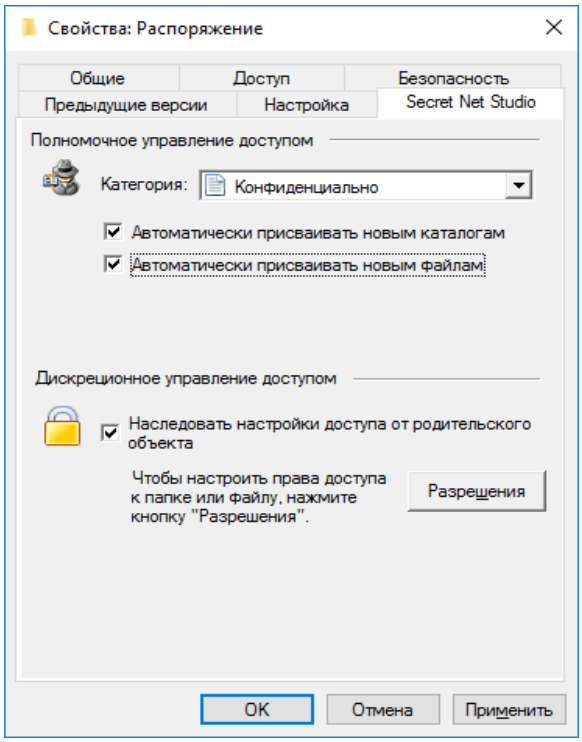
Команда	Описание
О системе	Предоставляет общую информацию о системе Secret Net Studio
Управление (для пользователя)	Вызывает локальный центр управления с правами учетной записи текущего пользователя. При выключенном механизме управления учетными записями (UAC) данная опция будет недоступна администратору

Команда	Описание
Управление (для администратора)	Вызывает локальный центр управления с правами встроенной учетной записи администратора компьютера. При выключенном механизме управления учетными записями (UAC) данная опция будет недоступна пользователю, не являющемуся администратором
Удаление данных	Содержит команду для безвозвратного затирания всей информации на локальных носителях (см. документ [**2**])
Ключи пользователя	Содержит команды для управления ключевой информацией пользователя, размещенной на ключевых носителях (см. документ [**2**])
Шифрование	Вызывает диалоговое окно полнодискового шифрования
Сбросить состояние тревоги	Выполняет сброс счетчиков событий тревоги (см. стр.**176**)
Уведомления о тревогах	Включает или отключает уведомления о событиях тревоги (см. стр.**176**)

Диалог "Secret Net Studio" в окне настройки свойств ресурса

Стандартное диалоговое окно настройки свойств ресурса (каталога или файла) ОС Windows содержит дополнительный диалог "Secret Net Studio". В диалоге выполняются действия по изменению категории конфиденциальности ресурсов для механизма полномочного управления доступом или прав доступа к ресурсам для механизма дискреционного управления доступом. Настройку может выполнять администратор безопасности или пользователи, являющиеся администраторами выбранного ресурса.

Вызов диалогового окна настройки свойств каталога или файла осуществляется стандартным способом в программе "Проводник". На рисунке представлен пример диалога "Secret Net Studio" в диалоговом окне настройки свойств каталога.



Программа настройки подсистемы полномочного управления доступом

Программа настройки подсистемы полномочного управления доступом предназначена для дополнительной настройки системы при необходимости использования режима контроля потоков. Также с помощью программы можно отключить вывод предупреждающих сообщений и регистрацию событий для случаев, когда такие оповещения не требуются.

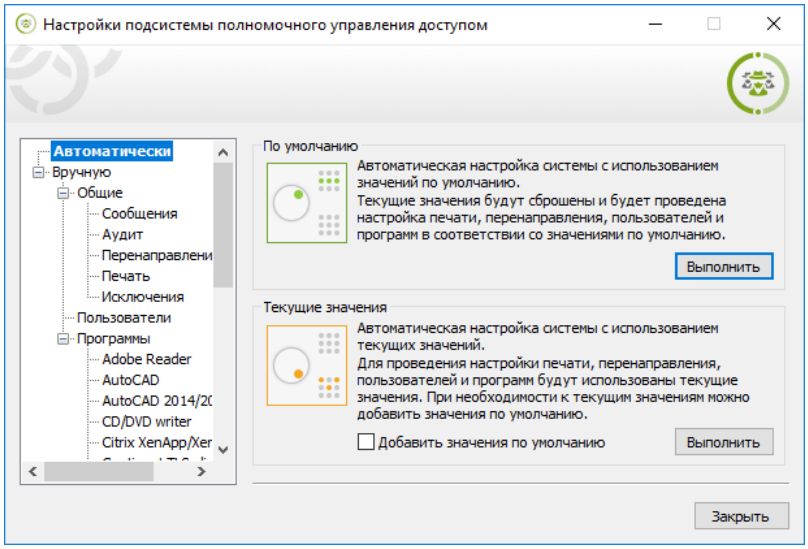
Для запуска программы:

- В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Программа настройки подсистемы полномочного управления доступом".

Внимание! Если включена функция контроля административных привилегий, на экране появится запрос PIN администратора.

- Для запуска программы в режиме администрирования введите PIN администратора безопасности и нажмите кнопку "ОК".
- Для запуска программы в режиме ограниченной функциональности нажмите кнопку "Отмена" или закройте окно запроса PIN администратора.

Пример содержимого окна программы представлен на рисунке ниже.



Настройка подсистемы полномочного управления доступом выполняется администратором.

Диалоговое окно "Управление Secret Net Studio" в Панели управления Windows

Диалоговое окно "Управление Secret Net Studio" предназначено для просмотра и редактирования общей информации о системе и для локального управления функционированием защитных механизмов и аппаратных средств защиты.

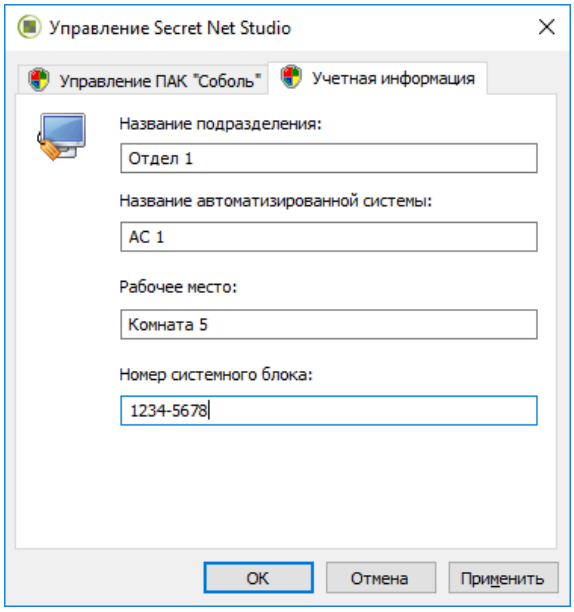
Для вызова диалогового окна:

- В Панели управления ОС Windows в категории "Система и безопасность" выберите элемент "Управление Secret Net Studio".

Внимание! Если включена функция контроля административных привилегий, на экране появится запрос PIN администратора.

- Для вызова диалогового окна в режиме администрирования введите PIN администратора безопасности и нажмите кнопку "ОК".
- Для отмены вызова диалогового окна нажмите кнопку "Отмена" или закройте окно запроса PIN администратора.

Пример содержимого диалогового окна представлен на рисунке ниже.



Средства для централизованного и локального управления

На рабочих местах администраторов для централизованной настройки и контроля работы защищаемых компьютеров используются средства централизованного управления. При запуске в соответствующем режиме эти средства могут использоваться и для локального управления непосредственно на защищаемых компьютерах. Например, для управления компьютером с установленным клиентом Secret Net Studio в автономном режиме функционирования.

В состав средств централизованного управления входят следующие программы:

- "Центр управления";
- "Управление пользователями";
- "Контроль программ и данных (централизованный режим)".

Примечание. В данном разделе перечислены регулярно используемые средства управления. Для выполнения частных специфических задач могут использоваться дополнительные программные средства, описание работы с которыми приводится отдельно.

Центр управления

Центр управления устанавливается как отдельный компонент ("Secret Net Studio — Центр управления") — для работы в централизованном режиме или как составная часть клиента Secret Net Studio ("Локальный центр управления") — для работы в локальном режиме.

При работе в централизованном режиме Центр управления предоставляет возможности управления защищаемыми компьютерами на рабочем месте администратора безопасности, мониторинга и просмотра журналов, поступивших на хранение в базу данных сервера безопасности. Для работы с программой необходимо выполнить подключение к серверу безопасности. Также предусмотрена возможность запуска без соединения с сервером безопасности — для работы с записями журналов, сохраненных в файлах.

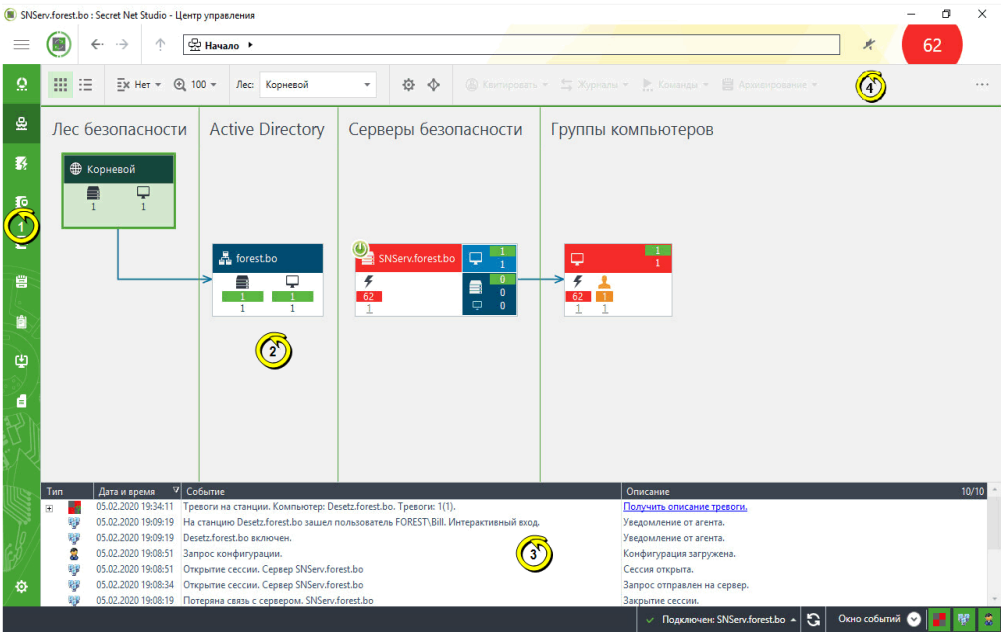
В локальном режиме работы доступны функции только локального управления компьютером, просмотра локальных журналов и журналов, сохраненных в файлах.

Для запуска Центра управления:

- В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Центр управления".

Перед началом работы на экране появляется стартовый диалог, предназначенный для выбора сервера безопасности, с которым будет установлено соединение.

На рисунке представлен пример основного окна Центра управления.



Для запуска Локального центра управления:

- В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Локальный центр управления".

Внимание! Если включена функция контроля административных привилегий, на экране появится запрос PIN администратора.

- Для запуска программы в режиме администрирования введите PIN администратора безопасности и нажмите кнопку "ОК".
- Для запуска программы в режиме ограниченной функциональности нажмите кнопку "Отмена" или закройте окно запроса PIN администратора.

Программа управления пользователями

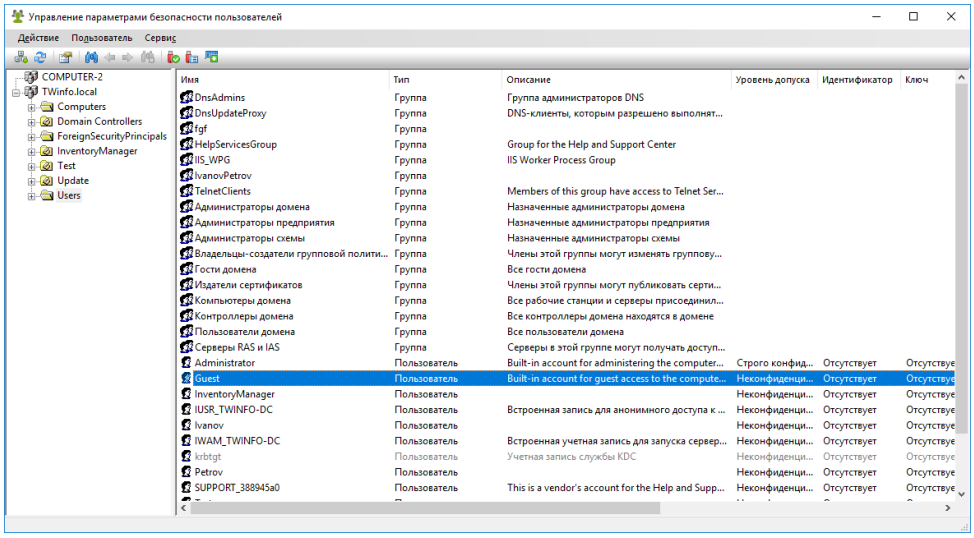
Программа управления пользователями, входящая в состав средств системы Secret Net Studio, предназначена для настройки параметров работы пользователей в системе защиты. В программе можно выполнять действия как с доменными пользователями, так и с локальными.

Для запуска программы:

- В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Управление пользователями".

Внимание! Если включена функция контроля административных привилегий, на экране появится запрос PIN администратора. Для запуска программы в режиме администрирования введите PIN администратора безопасности и нажмите кнопку "ОК".
Без ввода PIN администратора программа не будет запущена.

Пример содержимого окна программы представлен на рисунке ниже.



Интерфейс программы реализован аналогично стандартной оснастке ОС Windows "Active Directory — пользователи и компьютеры". В левой части окна отображается список контейнеров (текущий компьютер и структура разделов и организационных подразделений домена), а в правой — список пользователей в выбранном контейнере. Список пользователей представлен в виде таблицы со сведениями об уровнях допуска пользователей, наличии идентификаторов и криптографических ключей.

Если выбран параметр "Усиленная аутентификация по паролю", то для выполнения операций с пользователями необходимо будет выставлять отметку в поле "Синхронизировать данные пользователя на сервере аутентификации" при каждой операции либо выставить отметку в поле "Доверять аутентификации Windows" в Центре управления.

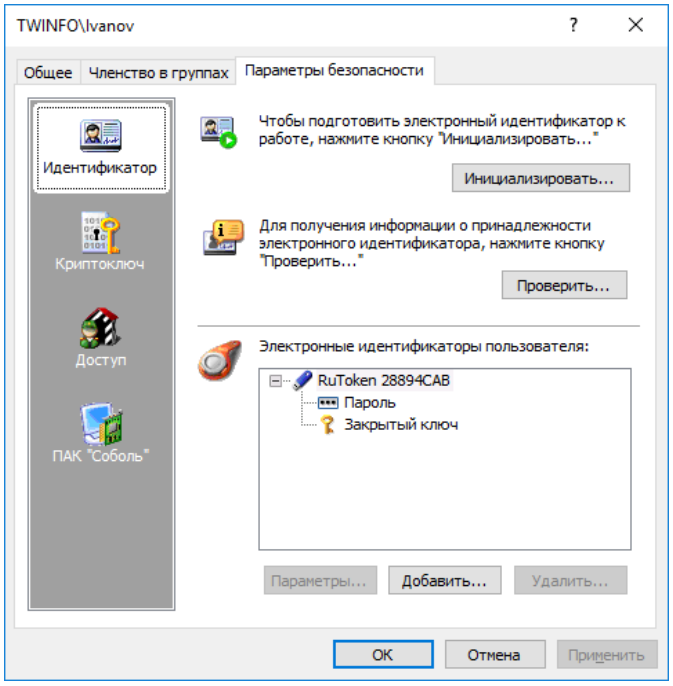
Для централизованного управления по умолчанию в программу загружается структура текущего домена. При необходимости можно загрузить структуры других доменов AD, если есть возможность подключения к этим доменам. Для этого используйте команду "Подключиться к домену Active Directory" в меню "Действие".

Совет. При работе с большим количеством объектов удобно использовать функции сортировки и поиска пользователей. Сортировка выполняется стандартными способами по содержимому колонок таблицы в списке пользователей. Поиск можно выполнять по различным критериям. Для настройки параметров поиска выберите команду "Поиск" в меню "Пользователь" и укажите нужные критерии в диалоге настройки. Результаты поиска выводятся в самом диалоге настройки, а также выделяются в списках пользователей после закрытия диалога. Для переходов между найденными объектами используйте команды "Следующий" и "Предыдущий" в меню "Пользователь".

Имеется возможность удаления из баз данных сервера аутентификации Secret Net Studio учетных записей пользователей, удаленных из AD, но оставшихся в базах Secret Net Studio. Для этого в меню "Сервис" выберите команду "Удаление потерянных пользователей".

Совет. Не рекомендуется удалять потерянных пользователей без крайней необходимости, в особенности в структуре с несколькими доменами AD (во избежание удаления пользователей из других доменов).

Управление параметрами пользователей для работы в системе Secret Net Studio осуществляется в диалоге "Параметры безопасности". Пример диалогового окна настройки свойств доменного пользователя представлен на следующем рисунке.



Программа "Контроль программ и данных"

Программа "Контроль программ и данных" предназначена для настройки механизмов КЦ и ЗПС. В ходе настройки для механизма контроля целостности определяются списки контролируемых объектов, методы и расписание проведения контроля, реакция системы на результат контроля. Для замкнутой программной среды определяются списки программ, запуск которых разрешен пользователям. Из этих сведений формируется модель данных, представляющая собой иерархию объектов и описание связей между ними.

Для работы с программой предусмотрены следующие режимы:

- локальный режим работы — используется для редактирования локальной модели данных на компьютере;
- централизованный режим работы — используется для редактирования централизованной модели данных с описаниями объектов, контролируемых на защищаемых компьютерах. Централизованная модель данных применяется на клиентах в сетевом режиме функционирования совместно с локальными моделями, если они заданы. При этом приоритет имеют параметры централизованной модели.

При централизованном управлении, если в системе присутствуют компьютеры с версиями ОС различной разрядности, формируются две модели данных — для компьютеров с 32-разрядными ОС и для компьютеров с 64-разрядными ОС. Администратор с помощью программы может редактировать только одну централизованную модель данных, разрядность которой совпадает с разрядностью версии ОС Windows компьютера администратора. Поэтому при необходимости редактирования централизованной модели другой разрядности администратору следует использовать компьютер с версией ОС той же разрядности.

Для запуска программы в централизованном режиме:

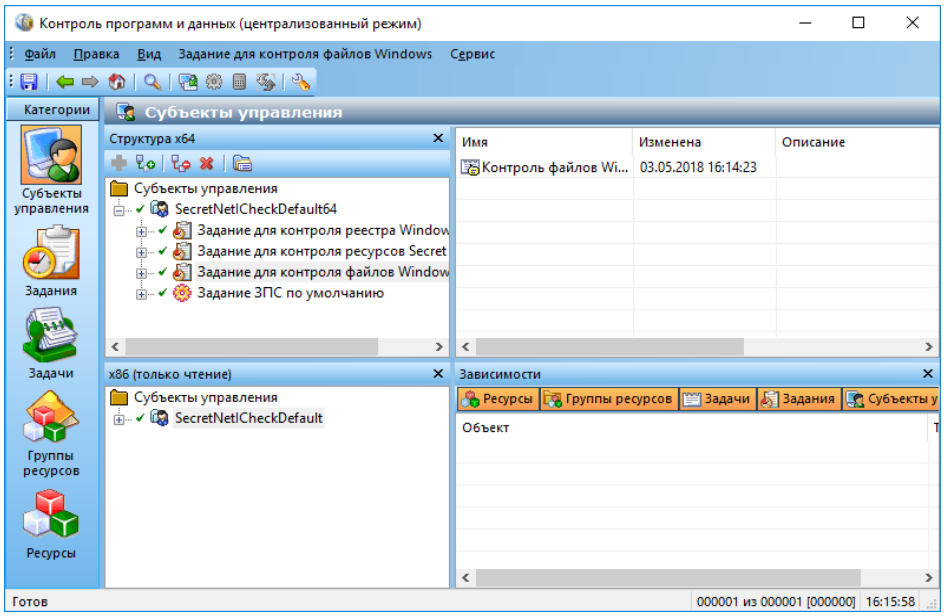
1. В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Контроль программ и данных (централизованный режим)".

   При запуске программа проверяет возможность полного доступа к модели данных соответствующей разрядности в ЦБД КЦ-ЗПС. Полный доступ возможен только с одного компьютера системы.

2. Если возможность полного доступа к ЦБД отсутствует (на другом компьютере с ОС той же разрядности уже работает Центр управления КЦ-ЗПС в централизованном режиме), на экране появится сообщение об этом с запросом дальнейших действий. Предусмотрены следующие варианты:
   - отменить запуск программы (рекомендуется) — для этого нажмите кнопку "Отмена";
   - запустить программу с доступом к ЦБД КЦ-ЗПС в режиме "только для чтения" — для этого нажмите кнопку "Нет". В этом случае в программу будет загружена последняя сохраненная в ЦБД модель данных. Возможность редактирования модели будет отсутствовать;
   - запустить программу и получить полный доступ к ЦБД — для этого нажмите кнопку "Да". Это приведет к тому, что пользователь, работающий с Центром управления КЦ-ЗПС на другом компьютере, потеряет возможность записи в ЦБД и сохранения сделанных изменений.

   Внимание! Если включена функция контроля административных привилегий, на экране появится запрос PIN администратора.
   - Для запуска программы в режиме администрирования введите PIN администратора безопасности и нажмите кнопку "ОК".
   - Для запуска программы в режиме ограниченной функциональности нажмите кнопку "Отмена" или закройте окно запроса PIN администратора.

На рисунке представлен пример содержимого окна программы в централизованном режиме.

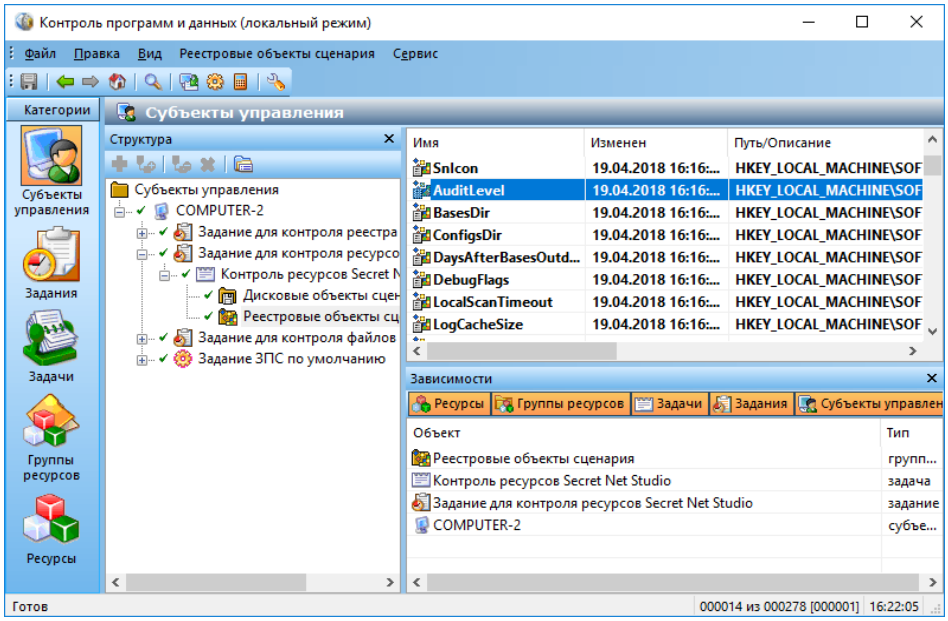


Для запуска программы в локальном режиме:

- В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Контроль программ и данных".

  Внимание! Если включена функция контроля административных привилегий, на экране появится запрос PIN администратора.
  - Для запуска программы в режиме администрирования введите PIN администратора безопасности и нажмите кнопку "ОК".
  - Для запуска программы в режиме ограниченной функциональности нажмите кнопку "Отмена" или закройте окно запроса PIN администратора.

На рисунке представлен пример содержимого окна программы в локальном режиме.


Контроль программ и данных (локальный режим)
Файл Правка Вид Реестровые объекты сценария Сервис
Категории
Субъекты управления
Задания
Задачи
Группы ресурсов
Ресурсы
Субъекты управления
Структура
Субъекты управления
COMPUTER-2
Задание для контроля реестра
Задание для контроля ресурсо
Контроль ресурсов Secret N
Дисковые объекты сцен
Реестровые объекты сц
Задание для контроля файлов
Задание ЗПС по умолчанию
Имя
Изменен
Путь/Описание
SnIcon 19.04.2018 16:16:... HKEY_LOCAL_MACHINE\SOF
AuditLevel 19.04.2018 16:16:... HKEY_LOCAL_MACHINE\SOF
BasesDir 19.04.2018 16:16:... HKEY_LOCAL_MACHINE\SOF
ConfigsDir 19.04.2018 16:16:... HKEY_LOCAL_MACHINE\SOF
DaysAfterBasesOutd... 19.04.2018 16:16:... HKEY_LOCAL_MACHINE\SOF
DebugFlags 19.04.2018 16:16:... HKEY_LOCAL_MACHINE\SOF
LocalScanTimeout 19.04.2018 16:16:... HKEY_LOCAL_MACHINE\SOF
LogCacheSize 19.04.2018 16:16:... HKEY_LOCAL_MACHINE\SOF
Зависимости
Ресурсы
Группы ресурсов
Задачи
Задания
Субъекты управлен
Объект
Тип
Реестровые объекты сценария групп...
Контроль ресурсов Secret Net Studio задача
Задание для контроля ресурсов Secret Net Studio задание
COMPUTER-2 субъе...
Готов
000014 из 000278 [000001] 16:22:05

Глава 12
Общие сведения о Центре управления

Для централизованного управления защищаемыми компьютерами используется отдельно устанавливаемый компонент "Secret Net Studio — Центр управления". Данный компонент предоставляет следующие основные возможности:

- настройка параметров защиты и управление компьютерами;
- мониторинг состояния системы;
- конфигурирование сетевой структуры системы Secret Net Studio;
- работа с централизованными журналами.

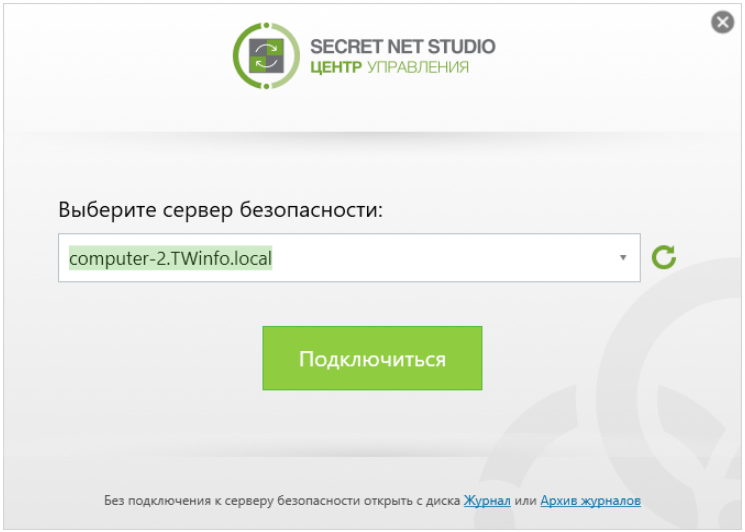
Примечание. В составе клиентского ПО системы Secret Net Studio устанавливается вариант Центра управления для работы в локальном режиме — Локальный центр управления. Режим предназначен для локальной настройки параметров защиты, управления механизмами и загрузки локальных журналов данного компьютера. Возможности централизованного управления в этом режиме недоступны.
В данной главе приведены сведения об использовании Центра управления для централизованного управления. Соответствующие функции для локального управления реализованы аналогично.

Запуск

Для запуска Центра управления:

1. В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Центр управления".

   На экране появится стартовый диалог программы.



2. В поле "Сервер безопасности" введите или выберите имя сервера безопасности, с которым будет установлено соединение. Для получения списка всех зарегистрированных серверов безопасности нажмите кнопку справа от поля (выполнение операции может занять длительное время).
3. Нажмите кнопку "Подключиться".

Примечание. Центр управления предусматривает возможность запуска без подключения к серверу безопасности — для просмотра содержимого журналов, сохраненных в файлах. Для открытия файлов используйте следующие команды в нижней части стартового диалога:

- "Журнал" — для загрузки журнала из файла;
- "Архив журналов" — для загрузки архива журналов из файла.

Интерфейс

Пример внешнего вида основного окна Центра управления представлен на рисунке ниже.

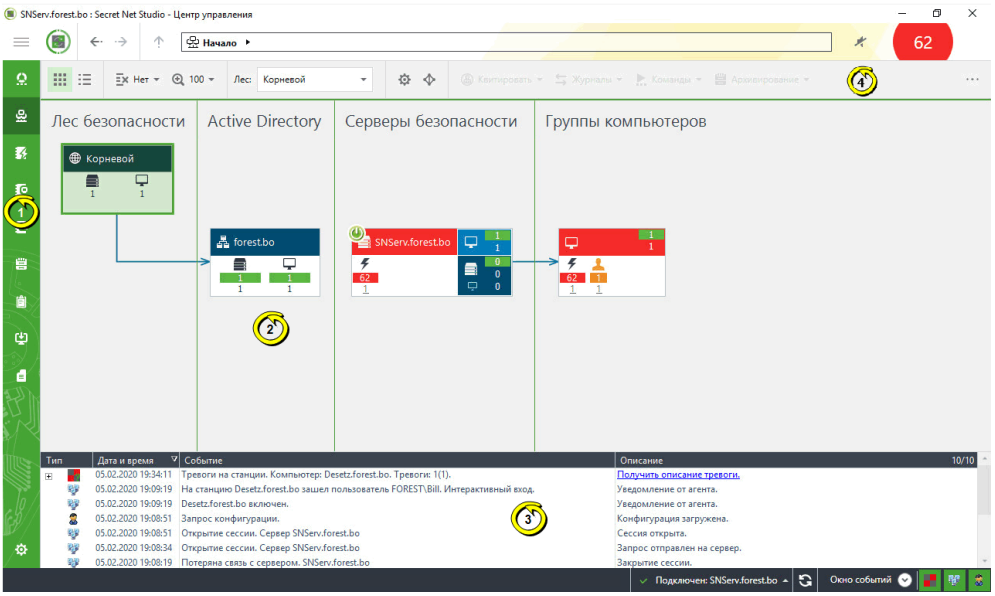


Рис.1 Пример окна Центра управления (панель "Компьютеры")

Пояснение. На рисунке обозначены: 1 — панель навигации по функциям Центра управления; 2 — панель "Компьютеры" в режиме "Диаграмма"; 3 — панель "События системы"; 4 — средства навигации по структуре ОУ.

Элементы интерфейса

Основное окно Центра управления состоит из следующих частей:

- панель навигации по функциям приложения (панель навигации) — отображается в левой части основного окна и содержит ярлыки вызова панелей управления, а также средств настройки программы;
- панели управления — предназначены для отображения сведений и выполнения действий с объектами.

В Центре управления имеются панели управления, приведенные в таблице ниже.

Статистика
Содержит сведения об общем состоянии защищенности системы
Компьютеры
Содержит средства администрирования и управления компьютерами
Журналы тревог
Содержит средства загрузки записей журнала событий тревоги
Журналы станций
Содержит средства загрузки записей журнала станций
Журналы сервера
Содержит средства загрузки записей журнала сервера безопасности
Архивы
Содержит средства загрузки архивов журналов

Отчеты
Содержит средства для работы с отчетами
Развертывание
Содержит средства настройки автоматической установки и обновления ПО на компьютерах
Паспорт ПО
Содержит средства контроля состава и целостности ПО на компьютерах

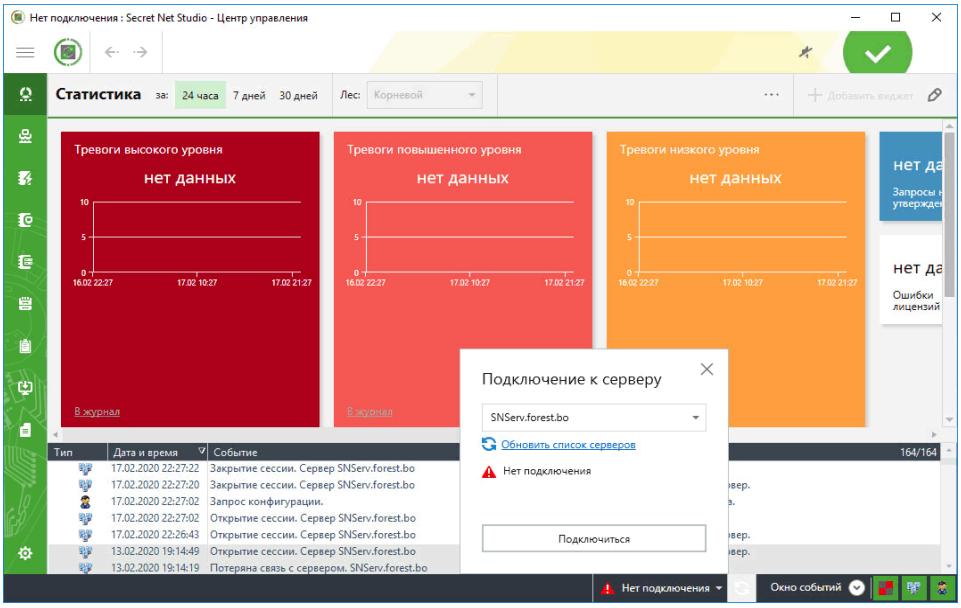
Подключение к серверу безопасности

Сеанс подключения к серверу безопасности начинается при открытии сессии. Если сессия с нужным сервером безопасности не была открыта при запуске Центра управления или потеряно соединение с сервером, подключиться к этому серверу можно без перезапуска. При необходимости подключения к другому серверу безопасности сначала выполняется команда разрыва соединения, после чего можно подключиться к нужному серверу.

Для открытия сессии:

1. В нижней части панели навигации (снизу в основном окне) нажмите кнопку "Нет подключения".

   На экране появится панель "Подключение к серверу".



2. В активном поле введите или выберите имя сервера безопасности, с которым будет установлено соединение. Для получения списка всех зарегистрированных серверов безопасности нажмите кнопку "Обновить список серверов", которая расположена ниже.
3. Нажмите кнопку "Подключиться".

   После установления соединения в программу будет загружена конфигурация с выбранного сервера.

Процедура закрытия сессии выполняется аналогично. Текущая открытая сессия автоматически закрывается при завершении работы Центра управления.

Настройка параметров работы

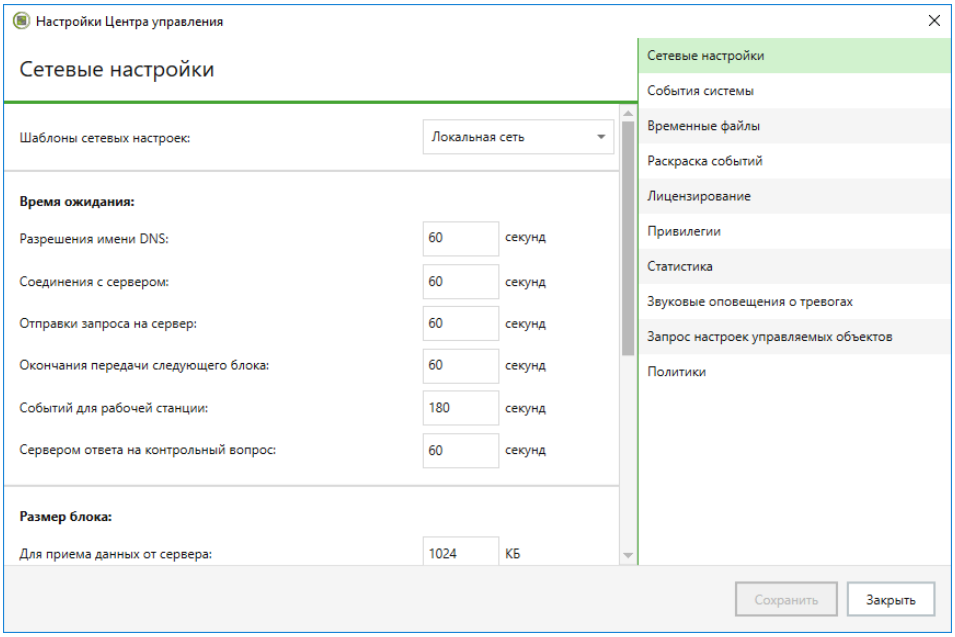
Для настройки параметров:

1. В нижней части панели навигации (слева в основном окне) нажмите кнопку "Настройки".

На экране появится панель средств настройки и конфигурирования.

2. Выберите ссылку "Настройки Центра управления".

   На экране появится одноименный диалог.



3. Укажите нужные значения для параметров. Параметры распределены по группам, которые перечислены в правой части диалога. Чтобы отобразить параметры нужной группы, выберите ее название. Описание параметров по группам приведено ниже.
4. После настройки параметров нажмите кнопку "Сохранить".

Примечание. Некоторые параметры вступают в силу со следующего запуска Центра управления.

Группа параметров "Сетевые настройки"

Содержит параметры сетевого взаимодействия Центра управления с сервером безопасности.

Поле "Шаблоны сетевых настроек"
Определяет шаблон настроек сетевого взаимодействия. Выберите нужный шаблон или настройте параметры вручную в остальных полях группы. Описание параметров см. на стр.**282**

Группа параметров "События системы"

Содержит параметры отображения данных в панели событий системы.

Поле "Количество событий в окне "События системы"
Определяет максимальное количество уведомлений, отображаемых в панели событий системы. При достижении заданного ограничения удаляется 80% старых уведомлений и в панели остается 20% последних поступивших уведомлений
Раздел "Раскраска событий"
Поля раздела определяют цвет фона строк таблицы в окне событий системы. В окне событий могут отображаться уведомления следующих типов: • "Сетевые события" — уведомления об изменении состояния объектов и наличии связи с сервером безопасности; • "Действия пользователя" — уведомления, информирующие о действиях пользователя Центра управления; • "События тревог" — уведомления о регистрации событий тревоги при работе с программой в централизованном режиме. Для каждого типа уведомлений можно задать особый цвет в соответствующей ячейке. Чтобы изменить текущий цвет, нажмите кнопку в правой части ячейки и выберите нужный цвет в появившемся диалоге

Группа параметров "Временные файлы"

Содержит параметры размещения и хранения временных файлов, создаваемых Центром управления.

Поле "Каталог для временных файлов"
Определяет путь к каталогу, в который помещаются временные файлы Центра управления. Чтобы указать другой каталог, введите полный путь к нему или нажмите кнопку справа и выберите нужный каталог в диалоге выбора объектов. Путь может быть задан в явном виде или с использованием переменных окружения
Поле "Время, по истечении которого удаляются временные файлы"
Определяет период хранения временных файлов в минутах с момента последнего обращения. Временные файлы загруженных журналов позволяют ускорить повторное обращение к этим журналам без необходимости новой загрузки данных с сервера. Параметр действует в течение сеанса работы пользователя с программой. При завершении работы с Центром управления временные файлы последнего сеанса удаляются независимо от заданного времени хранения
Поле "Путь к утилите PuTTY"
Определяет путь к файлу запуска программы удаленного управления PuTTY, используемой для подключения к компьютерам и отправки команд управления по протоколу Secure Shell (SSH). Программа PuTTY не входит в комплект поставки Secret Net Studio и устанавливается отдельно. Сведения о программе и ссылки для загрузки приведены на сайте разработчика: https://www.chiark.greenend.org.uk/~sgtatham/putty/ По умолчанию указан путь к каталогу установки Центра управления. Чтобы указать другой каталог, введите полный путь к нему или нажмите кнопку справа и выберите нужный каталог в диалоге выбора объектов

Группа параметров "Раскраска событий"

Содержит параметры цветового оформления записей журналов в зависимости от источников регистрации, категорий или кодов событий. Оформление осуществляется в соответствии с правилами, определяющими условия для содержимого полей в записях журналов. Описание настройки параметров см. на стр.**284**.

Группа параметров "Лицензирование"

Содержит параметры подключения к серверу активации лицензий.Secret Net Studio – С.

Поле "Сервер активации"	
Описание	**Значение по умолчанию**
Определяет IP-адрес сервера активации лицензий. Адрес сервера активации необходим для активации лицензий по сети.	Адрес: http://172.17.4.207 Порт: 8181
Поле "Таймаут запроса к серверу"	
Описание	**Значения**
Определяет время ожидания ответа сервера активации. В случае если активация лицензий прерывается по истечении времени ожидания, следует увеличить значение данного параметра.	1-900 с
Поле "Проверка ssl-сертификата среди отозванных"	
Определяет, должен ли ssl-сертификат проходить проверку среди отозванных. При снятии отметки активация лицензий по сети будет возможна даже если в системе не задан прокси.	
Поле "Настройки прокси"	
Определяет параметры использования прокси-сервера. Содержит следующие пункты: • Без прокси — Выберите данный пункт, если соединение с сервером активации лицензий происходит напрямую (без прокси-сервера); • Использовать системные настройки прокси — Используется автоматическое определение прокси-сервера (не рекомендуется); • Ручная настройка прокси-сервера — Выберите данный пункт, чтобы настроить прокси-сервер вручную. Укажите адрес прокси-сервера и порт. Если на прокси-сервере используется авторизация, укажите имя пользователя и пароль	

Группа параметров "Привилегии"

Содержит список привилегий для работы с Центром управления, которые предоставлены текущему пользователю (в том числе те привилегии, которые пользователь имеет от групп).

Группа параметров "Статистика"

Содержит поле, определяющее временной интервал обновления информации об общем состоянии защищенности системы на панели "Статистика".

Группа параметров "Звуковые оповещения о тревогах"

Содержит параметры звукового оповещения пользователя программы о возникновении событий тревоги. Управление режимом звукового оповещения осуществляется с помощью выключателя в соответствующем разделе панели средств настройки и конфигурирования.

Поле "Звуковой сигнал"
Определяет тип звукового сигнала, оповещающего о событиях тревоги. Для воспроизведения сигнала на компьютере должен быть установлен звуковой адаптер. Параметр может принимать значения: • "Тревога", "Сирена" — воспроизводится выбранный штатный звуковой сигнал; • *<имя_wav-файла>* — воспроизводится звуковой поток из заданного файла. Для вызова диалога выбора файла укажите значение "Выбрать..."
Поле "Количество повторов сигнала"
Определяет количество повторов звучания сигнала. Для ограничения количества повторов выберите нужное числовое значение. Если задано значение "бесконечно", сигнал будет повторяться до принудительного отключения

Поле "Интервал повторений"
Определяет паузу между повторами звукового сигнала

Группа параметров "Запрос настроек управляемых объектов"

Содержит поле, определяющее количество объектов, параметры которых после загрузки хранятся в оперативной памяти.

Группа параметров "Политики"

Содержит параметр, позволяющий настроить отображение типов поддерживаемых ОС для групповых политик. При установленной отметке для каждой групповой политики указана пиктограмма:

-  – политика поддерживается в ОС семейства Windows и/или
-  – политика поддерживается в ОС семейства Linux.

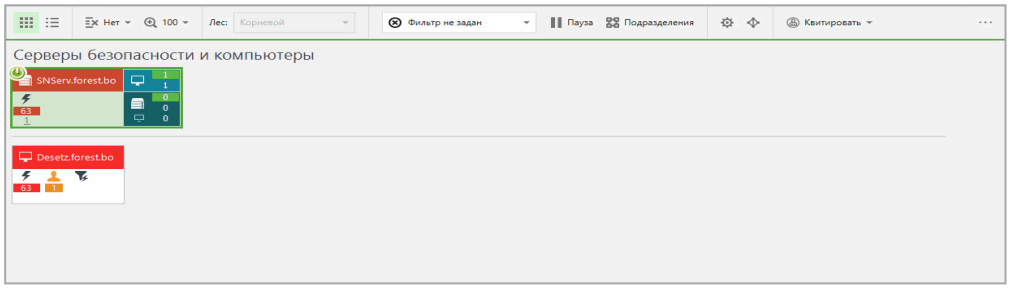
Глава 13
Структура централизованного управления

Диаграмма и список объектов управления

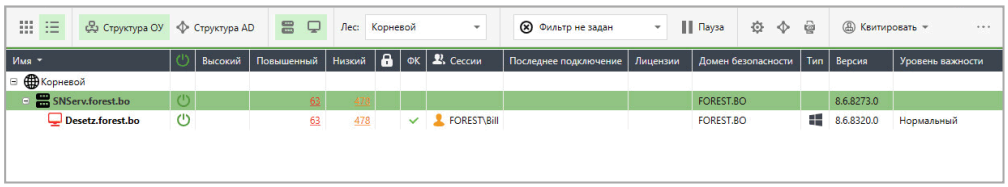
Для панели "Компьютеры" имеются следующие режимы отображения объектов управления:

- "Диаграмма" — режим предназначен для отображения в графическом виде сведений о структуре объектов управления;
- "Таблица" — режим предназначен для вывода иерархического списка объектов управления в табличном виде.

Пример режима диаграммы управления представлен на рисунке ниже.



Пример табличного режима отображения представлен на рисунке ниже.



Для переключения режимов отображения используются кнопки "Диаграмма" и "Таблица", расположенные в левом верхнем углу панели "Компьютеры".

Объекты структуры

Структура на диаграмме управления выводится в виде схемы элементов, соответствующих лесам безопасности, организационным подразделениям, серверам безопасности и защищаемым компьютерам. Схема базируется на структуре доменов и организационных подразделений в Active Directory.

В структуре могут быть представлены компьютеры, на которых установлено следующее ПО:

- компьютеры под управлением ОС семейства Windows — клиентское ПО системы Secret Net Studio;
- компьютеры под управлением ОС семейства Linux — средство защиты информации Secret Net LSP (версии 1.7 и выше).

Внимание! Для компьютеров с установленным ПО Secret Net LSP централизованное управление осуществляется в ограниченном объеме.

Для отображения схемы предусмотрены следующие основные режимы:

- режим общей начальной структуры — отображаются домены, организационные подразделения, серверы безопасности и подчиненные им группы компьютеров в соответствующих подразделениях;
- режим отображения списков компьютеров — отображаются выбранный сервер безопасности и списки компьютеров непосредственного подчинения.

В режиме общей начальной структуры слева отображаются структура лесов безопасности, структура доменов и организационных подразделений Active Directory, а справа — серверы безопасности и группы компьютеров, расположенные на уровне объектов AD, к которым они относятся. В каждой из частей между элементами схемы проведены связи от родительских элементов к дочерним с указанием направления в виде стрелки. Пример диаграммы управления в режиме общей начальной структуры см. на рисунке на стр.**122**.

Для перехода в режим отображения списков компьютеров наведите указатель на нужный сервер безопасности или группу компьютеров и дважды нажмите левую кнопку мыши. Будет включен режим отображения, при котором верхняя часть диаграммы содержит выбранный сервер безопасности с его подчиненными серверами (если они есть), а ниже представлены компьютеры, непосредственно подчиненные выбранному серверу. Пример диаграммы управления в этом режиме см. на рисунке на стр.**128**. Возврат в режим общей начальной структуры осуществляется с помощью средств навигации в верхней части основного окна.

Пиктограммы объектов на диаграмме управления перечислены в следующей таблице:

Пиктограммы	Описание
	Лес безопасности
	Домен или организационное подразделение
	Сервер безопасности
	Компьютер или группа компьютеров

Фильтрация объектов

Для ограничения количества отображаемых объектов можно использовать следующие возможности фильтрации:

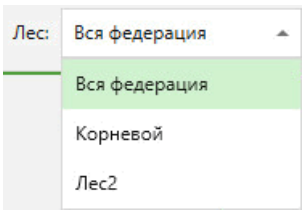
- фильтрация объектов по принадлежности лесам безопасности;
- фильтрация объектов по принадлежности доменам и организационным подразделениям;
- фильтрация компьютеров по их состоянию;
- фильтрация по типам объектов.

Фильтрация объектов по принадлежности к лесам безопасности

В режиме общей начальной структуры можно включить отображение только тех объектов, которые принадлежат определенному лесу безопасности либо всей федерации.

Для включения отображения объектов определенных лесов безопасности:

- В верхней части панели "Компьютеры" выберите из раскрывающегося списка лес безопасности, объекты которого необходимо отобразить.



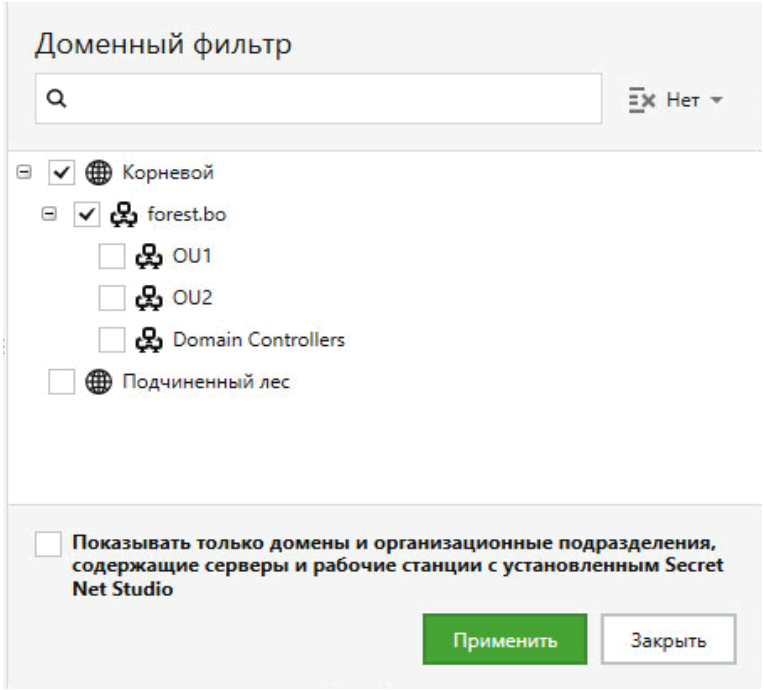
Фильтрация объектов по принадлежности доменам и организационным подразделениям

В структуре Active Directory могут присутствовать организационные подразделения или домены, объекты которых не требуется отображать в панели "Компьютеры". Например, такие организационные подразделения, в которых отсутствуют защищаемые компьютеры. При необходимости можно отключить отображение ненужных объектов с помощью фильтрации доменов и организационных подразделений. Фильтрация действует как для диаграммы управления, так и для табличного списка объектов.

Для включения отображения объектов определенных доменов и организационных подразделений:

1. В верхней части панели "Компьютеры" нажмите кнопку "Фильтр AD".

   На экране появится панель "Доменный фильтр" для выбора лесов, доменов и организационных подразделений, объекты которых должны присутствовать на диаграмме.



2. При необходимости в списке можно оставить только те домены и организационные подразделения, имена которых содержат определенную строку символов. Для этого введите искомую строку в верхнем поле.
3. Для управления списком отображаемых объектов используйте кнопку сортировки в верхней части панели.
4. Отметьте нужные элементы списка. Чтобы автоматически отметить только те домены и организационные подразделения, которые содержат компьютеры с установленным ПО Secret Net Studio, установите отметку в нижней части панели.
5. Нажмите кнопку "Применить" и затем кнопку "Закрыть", чтобы свернуть панель фильтра.

   На диаграмме управления будут отображены только те объекты, которые относятся к выбранным доменам и организационным подразделениям.

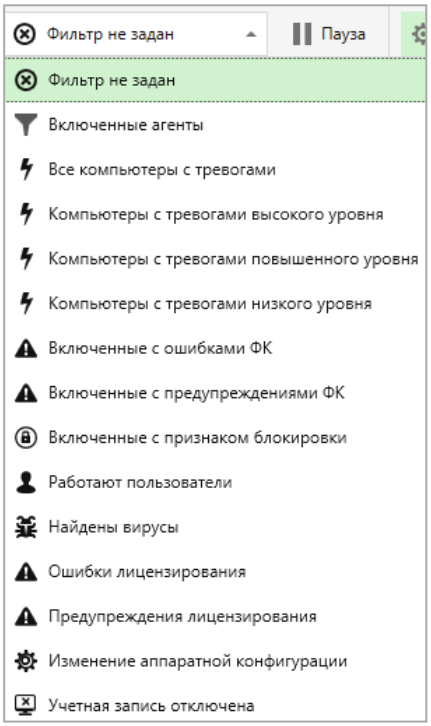
Фильтрация защищаемых компьютеров по их состоянию

В режиме отображения списков компьютеров (см. стр.**128**) можно включить отображение только тех объектов, которые имеют определенный признак состояния. Например, компьютеры с обнаруженными ошибками при проверке лицензий или компьютеры с признаком тревоги.

Для включения отображения компьютеров с определенным признаком состояния:

1. Включите режим отображения списков компьютеров. Для этого, например, подведите указатель к серверу/группе компьютеров и дважды нажмите левую кнопку мыши.
2. В верхней части панели "Компьютеры" выберите из раскрывающегося списка признак, по которому необходимо выполнить фильтрацию.

   Фрагмент панели со средствами фильтрации компьютеров представлен на рисунке ниже.



После включения фильтрации сервер безопасности в диаграмме управления обозначается специальной пиктограммой включенного фильтра. Данную пиктограмму можно использовать в качестве кнопки отключения фильтрации.

По умолчанию осуществляется динамическая фильтрация. То есть список автоматически обновляется при изменении состояния компьютеров. При необходимости можно отключить динамическую фильтрацию, чтобы зафиксировать текущий список компьютеров.

Для отключения динамической фильтрации:

- Нажмите кнопку "Пауза" рядом с выбранным признаком, по которому выполнена фильтрация.

  Динамическая фильтрация будет отключена и кнопка изменит свой вид. Чтобы снова включить фильтрацию, повторно нажмите кнопку.

Фильтрация по типам объектов

При отображении списка объектов в табличном виде можно фильтровать объекты с помощью следующих кнопок, расположенных над списком:

- "Структура ОУ" — включает представление иерархии объектов в виде дерева подчинения серверов безопасности и компьютеров (сервер подключения является корневым элементом иерархии);
- "Структура AD" — включает представление структуры домена Active Directory из компьютеров и организационных подразделений;
- "Отображение серверов" — включает и отключает отображение серверов безопасности;
- "Отображение компьютеров" — включает и отключает отображение защищаемых компьютеров.

Импорт и экспорт списка компьютеров

В режиме отображения списка компьютеров (см. стр. **128**) можно осуществить экспорт или импорт списка имен рабочих станций. Перед импортом списка компьютеров необходимо выполнить экспорт одного или нескольких компьютеров.

Для экспорта списка компьютеров:

1. В верхней части панели "Компьютеры" выберите режим отображения объектов управления "Таблица".

   На экране появится перечень корневых серверов безопасности и компьютеров.
2. Из списка компьютеров выберите элементы, информацию о которых необходимо экспортировать.
3. Нажмите кнопку "Экспортировать имена выбранных компьютеров в файл".

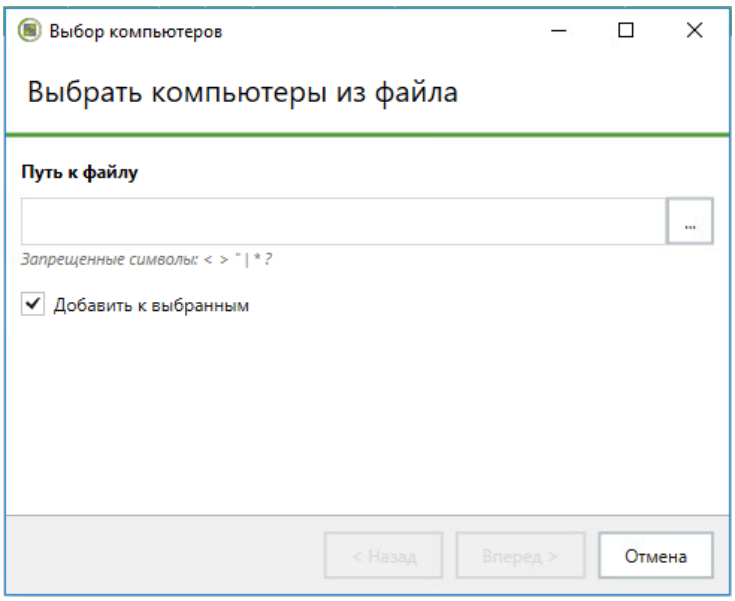
   В появившемся стандартном диалоге ОС введите имя файла и укажите место сохранения.
4. Нажмите кнопку "Сохранить".

   Файл будет сохранен с расширением ws.

Для импорта списка компьютеров:

1. В верхней части панели "Компьютеры" нажмите кнопку "Выбрать компьютеры из файла".

   На экране появится окно выбора компьютеров.



2. В поле "Путь к файлу" введите или выберите путь к файлу.
3. В появившемся стандартном диалоге выберите файл со списком компьютеров.

   Для экспорта поддерживаются файлы с расширением txt, csv, ws.
4. Нажмите кнопку "Открыть".

5. Поставьте отметку "Добавить к выбранным", если необходимо добавить новые компьютеры к имеющимся. Для формирования нового списка компьютеров отметка не ставится.
6. Нажмите кнопку "Вперед".

   При успешном добавлении компьютеров появится окно с информацией "Операция успешно завершена. Компьютеров добавлено:".
7. Нажмите кнопку "Готово".

Примечание. Если компьютеры частично не найдены, появится окно "Результат выбора компьютеров". Слева отобразятся выбранные компьютеры, а справа – не найденные в списке. В случае неудачи появляется окно "В указанном файле не найдено ни одного компьютера".

Управление отображением объектов

Для управления отображением объектов на диаграмме управления предусмотрены следующие общие возможности:

- переходы по структуре ОУ с помощью средств навигации;
- сортировка объектов;
- масштабирование структуры.

Дополнительно в режиме отображения списков компьютеров (см. стр.**128**) можно группировать объекты в соответствии с их принадлежностью организационным подразделениям.

Переходы по структуре ОУ с помощью средств навигации

Средства навигации по структуре ОУ (см. Рис.1 на стр.**122**) могут использоваться для переходов по структуре ОУ, а также для поиска нужных объектов. Переходы по структуре осуществляются посредством выбора элементов из числа представленных на диаграмме или из списка ранее выбранных элементов (в истории переходов). Поиск объектов осуществляется по именам при вводе искомой строки символов.

Методы работы со средствами навигации аналогичны используемым методам в стандартных приложениях ОС Windows Internet Explorer и Проводник.

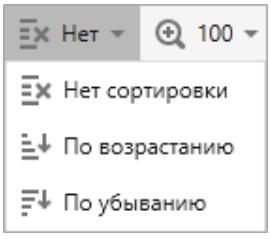
Сортировка объектов

Объекты на диаграмме можно сортировать в алфавитном порядке имен. Сортировка выполняется в прямом или обратном направлении.

Для сортировки объектов:

1. В верхней части панели "Компьютеры" раскройте меню сортировки.

   На экране появится меню выбора направления сортировки. Фрагмент панели после раскрытия меню представлен на следующем рисунке.



2. Выберите нужное направление сортировки.

   Объекты будут упорядочены в выбранном направлении.

Использование средств масштабирования диаграммы

Средства масштабирования предоставляют возможности отображения на диаграмме элементов в выбранном масштабе. За счет этого можно разместить на экране все необходимые элементы.

Для изменения масштаба отображения:

- В верхней части основного окна программы укажите нужный масштаб.

Группировка компьютеров по принадлежности организационным подразделениям

В режиме отображения списков компьютеров по умолчанию выводится общий список подчиненных компьютеров выбранного сервера безопасности. Если серверу безопасности подчинены компьютеры, входящие в различные организационные подразделения, можно включить группировку компьютеров. При включенной группировке список компьютеров разделяется на блоки, соответствующие различным подразделениям. Блоки отделяются горизонтальными линиями с указанием основных сведений о каждом блоке.

Примечание. В режиме отображения общей начальной структуры в диаграмме всегда действует группировка компьютеров в элементы, называемые группами компьютеров. Каждый такой элемент объединяет компьютеры, подчиненные одному серверу безопасности и входящие в одно организационное подразделение. Чтобы определить, какому серверу подчинены компьютеры из группы, найдите на диаграмме родительский элемент (от которого проведена связь к этой группе) или подведите указатель к элементу группы и дважды нажмите левую кнопку мыши, чтобы перейти в режим отображения списков компьютеров.

Для включения группировки списка компьютеров:

1. Включите режим отображения списков компьютеров. Для этого используйте средства навигации для перехода к нужным объектам (см. выше) или подведите указатель к серверу/группе компьютеров и дважды нажмите левую кнопку мыши.
2. В панели управления отображением объектов нажмите кнопку "Подразделения" ("Группировка по подразделениям").

   Список компьютеров будет разделен на блоки, соответствующие организационным подразделениям. Чтобы снова отключить группировку, повторно нажмите кнопку.

Структура управления после установки компонентов Secret Net Studio

Установку компонентов системы Secret Net Studio следует выполнять в порядке, описанном в главах 5–7 настоящего документа. Если при установке серверов безопасности и клиентов выполнялось их подчинение соответствующим серверам безопасности, компьютеры с этими компонентами будут включены в структуру оперативного управления. Структура ОУ считается сформированной на достаточном уровне, если все защищаемые компьютеры присутствуют в ней и подчинены серверам безопасности.

Для компьютеров под управлением ОС семейства Linux операции добавления в структуру ОУ и подчинения серверам безопасности недоступны до установки ПО Secret Net LSP. После установки ПО эти компьютеры могут участвовать в процессе редактирования структуры ОУ наравне с другими.

Редактирование структуры управления

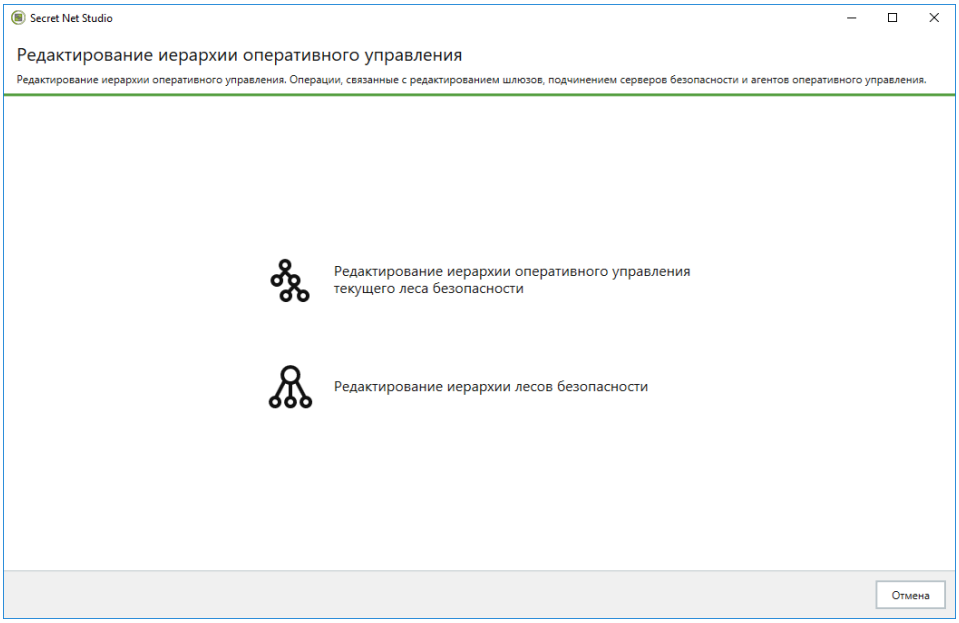
Для реализации функций централизованного управления в составе структуры ОУ должны присутствовать все имеющиеся серверы безопасности и защищаемые компьютеры. Операции добавления объектов в структуру ОУ и исключения из нее могут выполняться автоматически при установке или удалении ПО системы Secret Net Studio на компьютерах. При необходимости в Центре управления можно вручную добавить или удалить объекты в структуре. Например, для реализации автоматической установки клиентского ПО Secret Net Studio или для подчинения серверу безопасности компьютеров с установленным ПО Secret Net LSP, а также для регистрации шлюза, обеспечивающего взаимодействие с дочерним лесом доменов безопасности.

Для редактирования структуры ОУ:

1. В нижней части панели навигации (слева в основном окне) нажмите кнопку "Настройки".

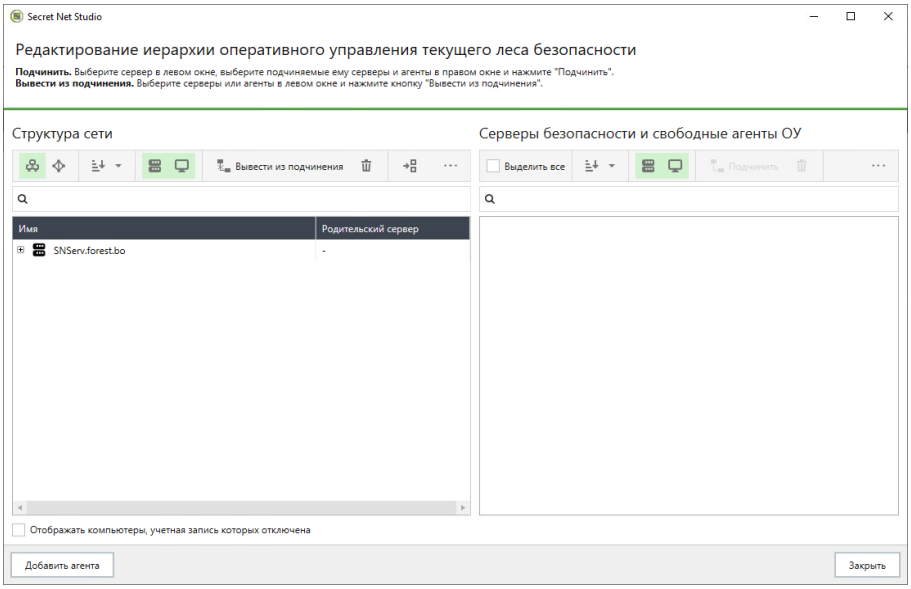
   На экране появится панель средств настройки и конфигурирования.
2. Нажмите кнопку "Конфигурирование".

   На экране появится диалог выбора режима редактирования.



3. Выберите вариант продолжения работы:
   - "Редактирование иерархии оперативного управления..." – если требуется приступить к редактированию структуры ОУ текущего леса безопасности.

     На экране появится диалог редактирования структуры ОУ.

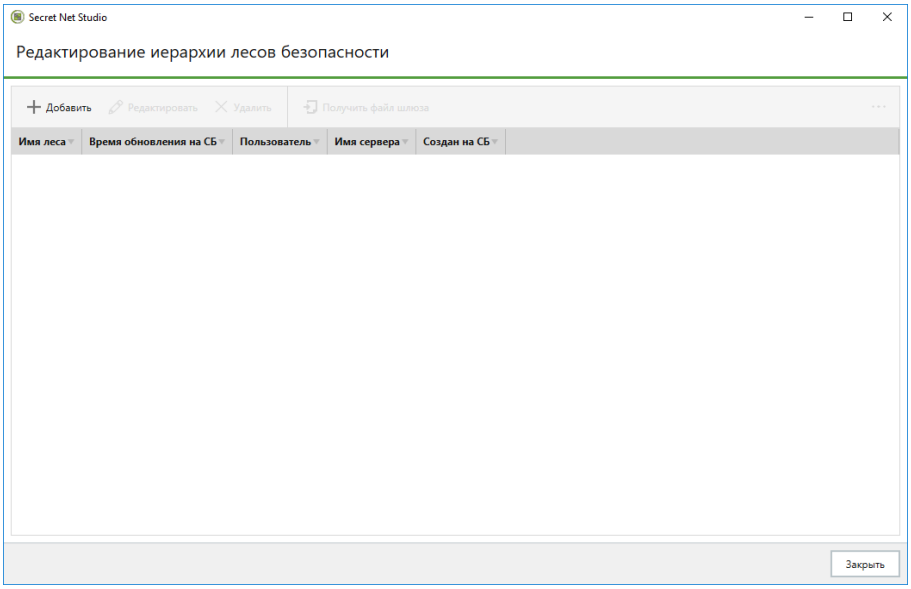


Текущая структура объектов управления представлена в левой части диалога. В правой части — список защищаемых компьютеров и серверов безопасности, доступных для подчинения выбранному серверу. Сформируйте структуру объектов (описание процедур см. ниже) и нажмите кнопку "Закрыть".

Примечание. При необходимости можно фильтровать списки объектов, исключая из отображения объекты определенных типов. Фильтрация выполняется с помощью соответствующих элементов над списками объектов (кнопки и поле ввода строки символов для поиска).

- "Редактирование иерархии лесов безопасности" – чтобы перейти к работе со списком шлюзов для подключения подчиненных лесов безопасности.

  На экране появится следующий диалог.



Диалог содержит список зарегистрированных шлюзов, для каждого из которых указан набор его параметров. Отредактируйте список шлюзов (см. стр.**140**) и нажмите кнопку "Закрыть".

Добавление объектов в структуру

В Центре управления можно добавить в качестве объекта структуры ОУ любой компьютер, зарегистрированный в Active Directory.

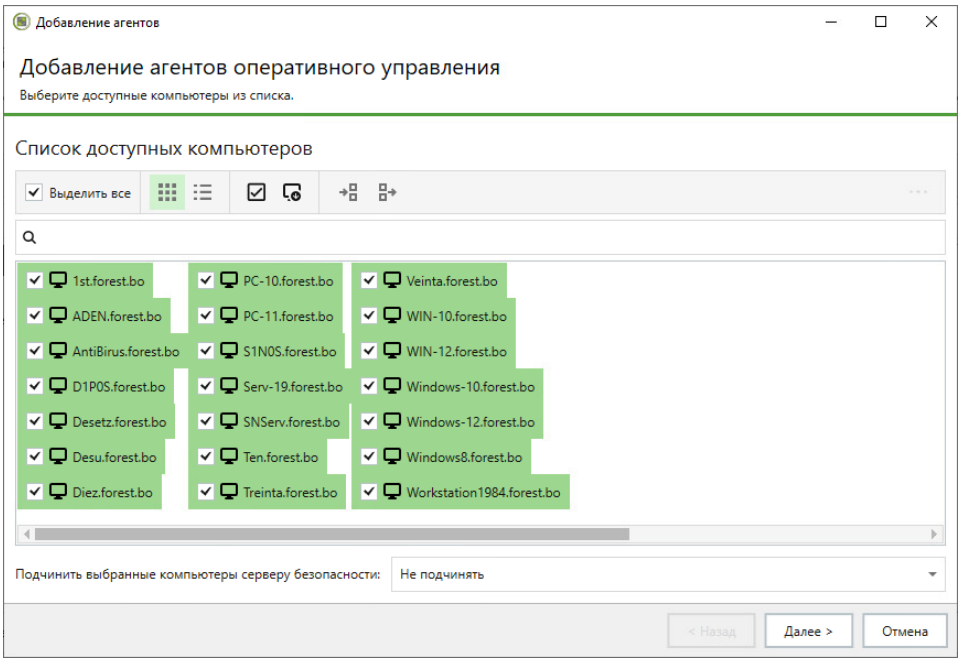
Примечание. Регистрация в Active Directory (включение в домен) компьютеров под управлением ОС семейства Linux, защищаемых средством защиты информации Secret Net LSP, осуществляется отдельно при настройке удаленного управления. Описание последовательности действий для настройки удаленного управления см. в документации Secret Net LSP.

Если домен безопасности сформирован на базе вложенного контейнера Active Directory (в организационном подразделении), перед добавлением в структуру ОУ компьютеры следует переместить в этот контейнер, используя штатные средства администрирования AD.

Для добавления компьютеров:

1. Вызовите диалог редактирования структуры ОУ (см. стр.**135**).
2. Нажмите кнопку "Добавить агент".

   На экране появится диалог с перечнем свободных компьютеров и имеющихся в структуре ОУ корневых серверов безопасности в раскрывающемся списке поля "Подчинить выбранные компьютеры серверу безопасности".



   Диалог содержит список компьютеров в контейнере AD, не входящих в структуру ОУ (рассматривается контейнер, на базе которого сформирован домен безопасности текущего сервера).

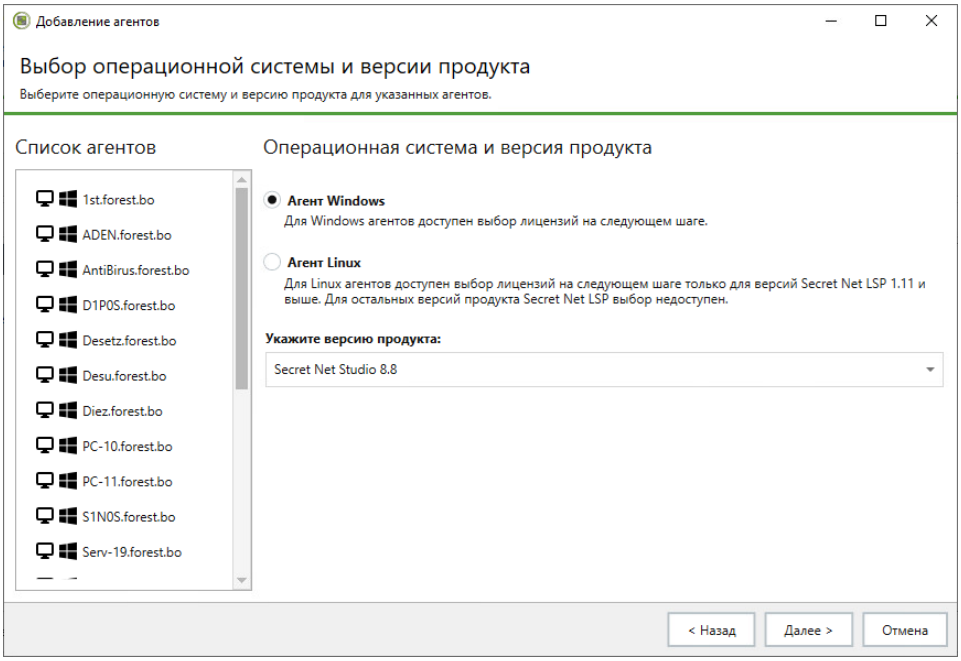
   Примечание. Список компьютеров может быть представлен в простой или табличной форме с помощью соответствующих кнопок, расположенных над списком. При необходимости можно фильтровать список, исключая из отображения отключенные учетные записи и/или не имеющие в названии заданную строку символов путем установки или удаления отметки в поле "Отображать компьютеры, учетная запись которых отключена".

3. Отметьте в списке компьютеры, которые нужно добавить в структуру.
4. Чтобы подчинить компьютеры серверу безопасности, выберите имя нужного сервера в поле "Подчинить выбранные компьютеры серверу безопасности".

   Примечание. Подчинение компьютеров можно выполнить позже (см. стр.**140**).

5. Нажмите кнопку "Вперед".

   На экране появится диалог для выбора операционной системы и версии продукта.

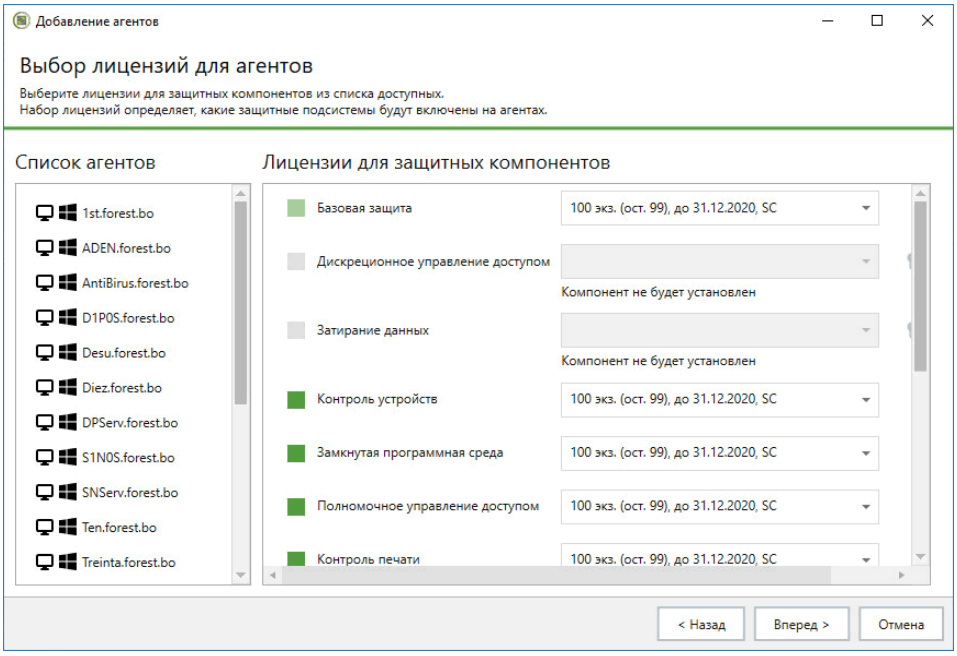


6. Укажите тип операционной системы, под управлением которой работают выбранные компьютеры, и версию используемого на них продукта.

Внимание! Необходимо корректно указать версию продукта для добавляемых компьютеров. В случае неправильно заданного значения стабильное функционирование добавленных компьютеров в контуре управления будет невозможно. В этом случае потребуется удалить и заново добавить эти объекты в структуру ОУ.

7. Нажмите кнопку "Вперед".

Если указан Агент Windows, на экране появится диалог выбора лицензий на использование компонентов (подсистем) Secret Net Studio на компьютерах.

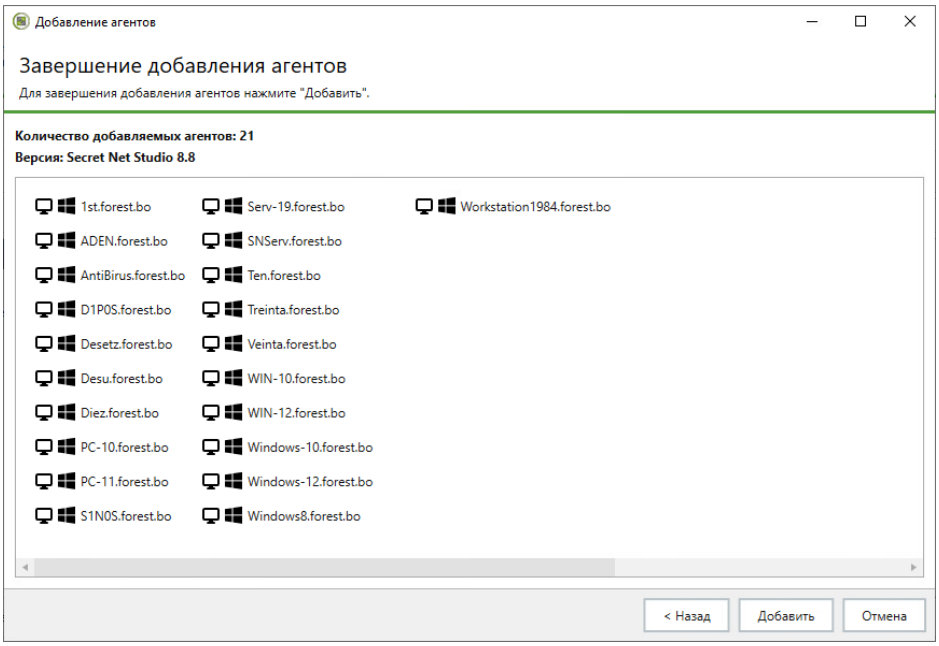


8. Отметьте подсистемы, которые будут функционировать. Для управления активацией подсистем (включение и отключение действия лицензий) используйте элементы управления, расположенные слева от названий подсистем. Если на сервере безопасности зарегистрированы различные лицензии для подсистемы, выберите нужную лицензию в раскрывающемся списке.

Пояснение. Подсистема "Базовая защита" устанавливается по умолчанию. Остальные подсистемы можно установить по выбору.

9. Нажмите кнопку "Вперед".

   На экране появится завершающий диалог.



10. Нажмите кнопку "Добавить".

    Выбранные компьютеры будут добавлены в текущую структуру ОУ.

Управление отношениями подчиненности в структуре ОУ

В структуре ОУ можно изменять отношения подчинения между серверами безопасности или подчинять защищаемые компьютеры другим серверам. Переподчинение объектов (например, при пересмотре сетевой структуры) требует предварительного выполнения процедуры вывода из подчинения этих объектов текущим серверам безопасности.

Вывод объектов из подчинения

При выводе объекта из подчинения текущему серверу безопасности этот объект становится свободным. Свободный компьютер в дальнейшем необходимо подчинить соответствующему серверу безопасности. Если из подчинения выведен сервер безопасности, этот компонент может продолжать функционировать в качестве независимого объекта управления.

Для вывода объектов из подчинения:

1. Вызовите диалог редактирования структуры ОУ (см. стр.**135**).
2. В списке "Структура сети" (слева) выберите объекты, которые необходимо вывести из подчинения.
3. Нажмите кнопку "Вывести из подчинения". В появившемся диалоге запроса подтвердите выполнение операции.

   Выбранные объекты будут представлены в списке свободных объектов при выборе сервера безопасности.

Подчинение объектов серверу безопасности

Подчинение новых объектов серверу безопасности выполняется из числа свободных серверов безопасности и защищаемых компьютеров. Если нужный сервер безопасности или защищаемый компьютер отсутствует в списке свободных объектов, перед подчинением необходимо добавить объект в структуру (см. стр.**137**) или вывести его из подчинения другому серверу безопасности (см. выше).

Для подчинения объектов:

1. Вызовите диалог редактирования структуры ОУ (см. стр.**135**).
2. В списке "Структура сети" (слева) выберите сервер безопасности, в подчинение которому необходимо добавить новые объекты.

   В правой части диалога будет выведен список свободных защищаемых компьютеров и корневых серверов, имеющихся в структуре ОУ.
3. В списке объектов правой части диалога отметьте компьютеры, которые нужно подчинить выбранному серверу безопасности. Чтобы установить отметки для всех элементов списка, отметьте поле "Выделить все", расположенное над списком.
4. Нажмите кнопку "Подчинить".

Удаление объектов из структуры ОУ

Процедуру удаления защищаемых компьютеров из структуры ОУ в Центре управления следует выполнять только в случае неработоспособности компонентов на этих компьютерах. Например, из-за некорректного завершения процедуры удаления ПО Secret Net Studio или при необходимости переноса компьютера из одного домена безопасности в другой. Если требуется временно исключить объект, следует вывести этот объект из подчинения серверу безопасности (см. стр.**139**), чтобы впоследствии заново установить отношения подчинения.

Для удаления объектов:

1. Вызовите диалог редактирования структуры ОУ (см. стр.**135**).
2. Выберите объекты для удаления в левом или правом списке.
3. Нажмите кнопку "Удаление объекта оперативного управления" над списком, в котором выбраны объекты.
4. В появившемся диалоге запроса подтвердите выполнение операции.

Управление шлюзами

В этом режиме работы мастер конфигурирования позволяет добавлять в структуру ОУ шлюзы, изменять их имена, удалять шлюзы, а также создавать для шлюзов специальный файл конфигурации, необходимый для установки шлюза в подчиненном лесу безопасности.

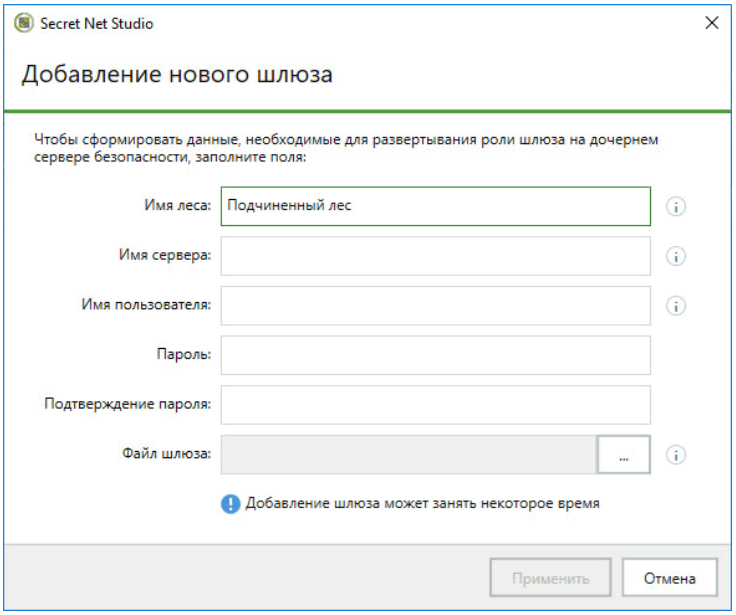
Добавление шлюза

При добавлении шлюза определяются его основные параметры и создается специальный файл, необходимый для установки ПО шлюза на дочернем сервере безопасности.

Для добавления шлюза:

1. Вызовите диалог редактирования списка шлюзов (см. стр.**135**).
2. Нажмите кнопку "Добавить".

   На экране появится диалог добавления шлюза.

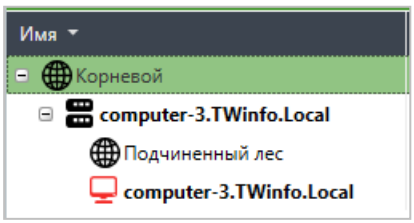


3. В полях диалога укажите параметры добавляемого шлюза.

Параметр	Описание
Имя леса	Под этим именем в структуре ОУ будет отображаться корневой объект, соответствующий дочернему лесу безопасности. Это имя в дальнейшем можно будет изменить
Имя сервера	DNS-имя компьютера с дочерним сервером безопасности, на котором будет функционировать данный шлюз. Требуется указать полное DNS-имя, включающее имя домена AD, например, SecServer.SecondDomain
Имя пользователя	Имя служебной учетной записи пользователя, необходимой для организации взаимодействия данного шлюза и корневого сервера безопасности. Использование этой учетной записи осуществляется в автоматическом режиме
Пароль, Подтверждение пароля	Введите и повторите ввод пароля для указанного пользователя. Запомните этот пароль, так как его потребуется указать при установке ПО шлюза на дочернем сервере безопасности
Файл шлюза	Имя файла, в котором будут сохранены параметры данного шлюза. Файл потребуется при установке ПО шлюза на дочернем сервере безопасности. Чтобы создать файл, нажмите кнопку справа от поля и укажите имя файла и его местоположение в появившемся стандартном диалоге

4. Нажмите кнопку"Применить".

   Начнется процесс добавления шлюза, занимающий некоторое время. Информация о ходе этого процесса отображается в виде сообщений в панели событий системы. Дождитесь его завершения и появления в списке шлюзов нового объекта. После этого в иерархическом списке ОУ также появится новый объект — подобно тому, как это показано на следующем рисунке.



5. Нажмите кнопку"Закрыть" в диалоге редактирования списка шлюзов.

После этого можно перейти к установке ПО шлюза на дочернем сервере безопасности и выполнить настройку параметров синхронизации для данного шлюза (см. ниже).

Редактирование списка шлюзов

Редактирование списка шлюзов осуществляется с помощью следующих кнопок.

Кнопка	Описание
Редактировать	Вызывает диалог редактирования имени шлюза для выбранного в списке элемента. Внесите нужны изменения и нажмите кнопку "Применить". Изменение других параметров шлюза возможно только путем его повторного создания.
Удалить	Удалить выбранные шлюзы из списка, из структуры ОУ и из базы данных сервера безопасности. После этого дальнейшее использование данных шлюзов будет невозможно. Для выбора нескольких элементов используйте вместе с мышью клавиши "Shift" и "Ctrl".
Получить файл шлюза	Повторно создать для выбранного шлюза специальный файл с его параметрами. В появившемся диалоге нажмите кнопку справа от поля и укажите имя файла и его местоположение в стандартном диалоге

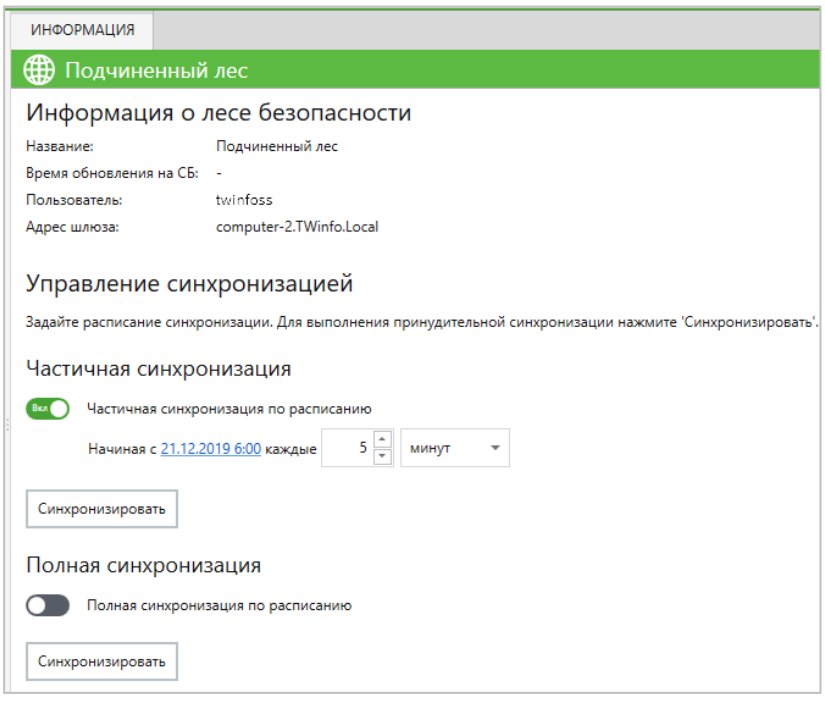
Настройка параметров синхронизации

Параметры синхронизации шлюза определяют объем и периодичность получения корневым сервером информации о состоянии объектов управления в дочернем лесу безопасности. Синхронизация может выполняться в двух режимах:

- Частичная синхронизация — обеспечивает синхронизацию только тех данных, которые изменились с момента выполнения последней синхронизации;
- Полная синхронизация — выполняется синхронизация всех без исключения данных о состоянии объектов управления.

Для настройки параметров синхронизации:

1. В Центре управления в панели "Компьютеры" выберите объект, соответствующий нужному дочернему лесу безопасности (шлюзу), для которого необходимо настроить параметры синхронизации. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств появится вкладка "Информация".



2. В группах полей "Частичная синхронизация" и "Полная синхронизация" переведите в нужное положение выключатель, включающий (положение "Вкл") или отключающий соответствующий режим синхронизации.
3. Для включенных режимов укажите дату начала выполнения синхронизации и ее периодичность в нужных единицах изменения времени.
4. Для сохранения изменений нажмите кнопку "Применить" внизу вкладки "Информация".

Совет. Если требуется немедленно выполнить синхронизацию в нужном режиме, используйте кнопки "Синхронизировать" в соответствующей группе полей. Кроме того, для выполнения принудительной синхронизации можно использовать команды из подменю "Лес" в контекстном меню объекта управления, соответствующего дочернему лесу безопасности.

Глава 14
Настройка параметров безопасности

В Secret Net Studio реализованы следующие функции управления параметрами безопасности:

- настройка параметров безопасности вручную;
- применение параметров безопасности из шаблона;

> **Примечание.** В Secret Net Studio имеются шаблоны параметров безопасности, настроенных в соответствии с требованиями о защите информации для различных информационных систем. Перечни требований приведены на стр.224.

- создание шаблона параметров безопасности по параметрам объекта;
- сравнение параметров безопасности объекта с параметрами безопасности из шаблона.

Списки параметров безопасности

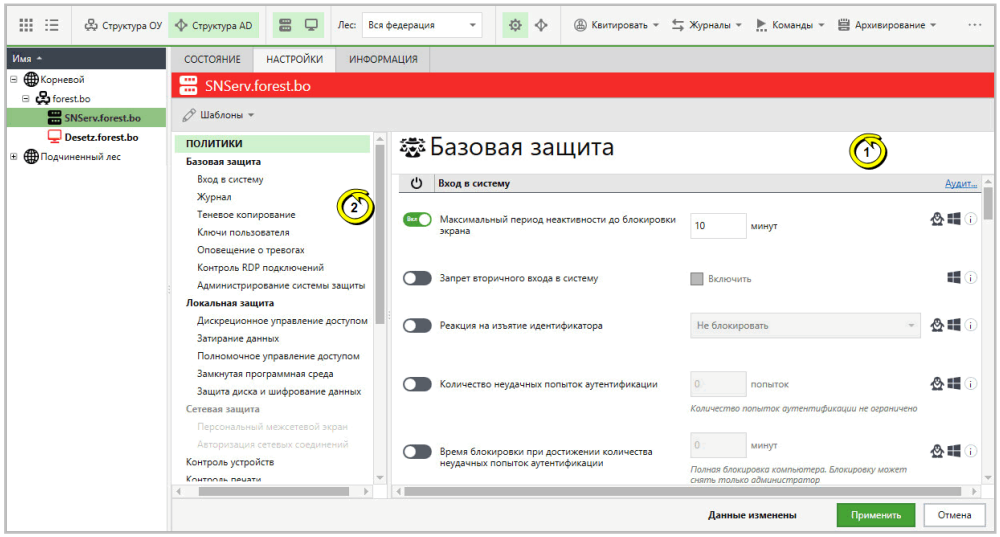
Управление параметрами безопасности осуществляется в панели "Компьютеры". Выберите нужный объект в структуре управления и включите отображение панели свойств объекта одним из следующих способов:

- нажмите кнопку "Свойства" на панели в верхней части окна;
- вызовите контекстное меню объекта и выберите команду "Свойства".

В панели свойств перейдите на вкладку "Настройки".

Для управления параметрами безопасности выбранного объекта необходимо загрузить параметры. Для этого перейдите на вкладку "Настройки" и нажмите кнопку "Загрузить настройки". Набор доступных параметров зависит от типа выбранного объекта. После загрузки параметров для их обновления используйте кнопку "Обновить" в верхней части вкладки.

Пример содержимого вкладки "Настройки" представлен на рисунке ниже.



> **Пояснение.** На рисунке обозначены: 1 — область отображения параметров; 2 — область оглавления.

Назначение элементов приведено в таблице ниже.

Область отображения параметров
Предназначена для просмотра и настройки параметров объектов. Параметры распределены по группам. Выбор группы с нужными параметрами осуществляется в области оглавления
Область оглавления
Предназначена для выбора разделов и групп для области отображения параметров. Оглавление содержит следующие разделы верхнего уровня: • "Политики" — объединяет группы параметров для настройки функционирования механизмов защиты на компьютерах; • "Регистрация событий" — объединяет группы параметров для настройки регистрации событий в локальных журналах; • "Параметры" — объединяет группы параметров для настройки и обслуживания серверов безопасности и защищаемых компьютеров

Области отображения разделены между собой передвигаемыми границами. При необходимости можно скрыть какую-либо область, передвинув ее границу. Для просмотра данных в каждой области используются отдельные средства прокрутки.

Сохранение изменений

Сделанные изменения в Центре управления вступают в силу после сохранения. Сохранение изменений возможно при активном сеансе связи с сервером безопасности. В процессе работы с Центром управления рекомендуется регулярно сохранять сделанные изменения, чтобы избежать их потери в случае разрыва соединения с сервером.

Для сохранения изменений используйте кнопку "Применить" в нижней части вкладки. Кнопка появляется при наличии несохраненных изменений.

Уведомление о результатах выполнения действия выводится в панели событий системы.

Настройка параметров в разделах "Политики" и "Регистрация событий"

В разделах "Политики" и "Регистрация событий" подразделений и серверов безопасности представлены параметры, которые применяются на компьютерах посредством групповых политик. Параметры предназначены для настройки функционирования механизмов защиты и регистрации событий в локальных журналах.

Параметры раздела "Политики"

Примечание. В данном разделе приведены перечни параметров для клиентов с ОС семейства Windows. Перечни параметров для клиентов с ОС семейства Linux различаются. В Центре управления можно настроить отображение ОС, поддерживаемых групповыми политиками (см. стр. 127).

В состав раздела "Политики" входят следующие группы параметров:

- группы базовой защиты ("Вход в систему", "Журнал", "Теневое копирование", "Ключи пользователя", "Оповещение о тревогах", "Контроль RDP подключений", "Администрирование системы защиты") — объединяют параметры функционирования механизмов базовой защиты клиента;
- группы защиты локальных ресурсов ("Дискреционное управление доступом", "Затирание данных", "Полномочное управление доступом", "Замкнутая программная среда", "Защита диска и шифрование данных", "Полнодисковое шифрование", "Хранение данных восстановления") — объединяют параметры функционирования механизмов локальной защиты клиента;

- группы защиты сетевых подключений ("Персональный межсетевой экран", "Авторизация сетевых соединений") — объединяют параметры функционирования механизмов сетевой защиты клиента;
- группа "Контроль устройств" — содержит параметры функционирования механизмов контроля подключения и изменения устройств и разграничения доступа к устройствам;
- группа "Контроль печати" — содержит параметры для настройки маркировки документов, теневого копирования, списка используемых принтеров и политик прямой печати;
- группа "Паспорт ПО" — содержит параметры настройки сбора данных СПС по расписанию, выбранных каталогов и расширения файлов.

Сведения о настройке механизмов приведены в соответствующих главах.

Если для механизма предусмотрена возможность управления регистрацией событий, можно выполнить переход к параметрам в разделе "Регистрация событий", относящимся к этому механизму. Для перехода к соответствующей группе параметров регистрации используйте ссылку "Аудит..." в правой части заголовка группы.

Параметры раздела "Регистрация событий"

Параметры раздела "Регистрация событий" предназначены для включения и отключения регистрации определенных событий в журнале Secret Net Studio. Параметры распределены по группам, соответствующим категориям событий.

Порядок применения параметров на компьютерах

Применение параметров, заданных в разделах "Политики" и "Регистрация событий", осуществляется на компьютерах в следующей последовательности:

1. Параметры, заданные непосредственно для компьютера (параметры локальной политики).
2. Параметры, заданные для доменов и организационных подразделений, — аналогично механизму групповых политик Windows сначала применяются параметры доменных политик и затем параметры политик для организационных подразделений.
3. Параметры, заданные для серверов безопасности, — сначала применяются параметры сервера, которому компьютеры подчинены непосредственно, а затем вышестоящих серверов по иерархии.

Таким образом, параметры политик, заданные для корневого сервера безопасности, имеют наивысший приоритет и применяются на всех компьютерах, которые находятся в непосредственном или транзитивном подчинении.

По умолчанию параметры заданы только в локальной политике. Для большинства параметров локальной политики изменение значений возможно как централизованно в Центре управления, так и локально на защищаемом компьютере. При этом изменить в локальной политике значение, заданное политикой другого уровня, невозможно. Сведения о политике, определяющей значение параметра, представлены в локальной политике в колонке "Источник".

При использовании нескольких серверов безопасности, если развернута структура доменов безопасности на базе родительских и вложенных контейнеров AD (например, один домен безопасности представляет весь домен AD, а другой — вложенное организационное подразделение в этом домене AD), действуют следующие особенности применения параметров политик:

- параметры политик доменов и организационных подразделений, заданные при подключении программы к серверу в родительском домене безопасности, не применяются на защищаемых компьютерах, которые подчинены серверу другого домена безопасности во вложенном контейнере Active Directory. Для этих компьютеров параметры политик доменов/организационных подразделений необходимо задать при подключении программы к серверу безопасности во вложенном контейнере AD. То есть в каждом домене безопасности используются отдельные наборы параметров для доменов/организационных подразделений;
- параметры политик для сервера безопасности являются уникальными в пределах леса доменов безопасности и могут быть заданы при подключении Центра управления как непосредственно к этому серверу, так и к любым серверам в других доменах безопасности (при наличии соответствующих прав). То есть параметры политик для сервера безопасности будут представлены одним набором независимо от того, как они были заданы — при подключении к этому серверу или к серверам других доменов безопасности.

Настройка параметров в разделе "Параметры"

В разделе "Параметры" представлены группы параметров, применяемых на выбранном сервере безопасности или защищаемом компьютере.

Параметры объектов могут быть представлены в следующих группах:

- "Сетевые настройки" — содержит параметры сетевых соединений при взаимодействии объекта с родительским сервером безопасности;
- "Сбор журналов" — содержит параметры передачи локальных журналов на сервер безопасности;
- "Конфигурация сервера" — содержит информацию о сертификате сервера безопасности и расположении временных файлов и архивов на сервере;
- "Архивирование журналов" — содержит параметры автоматического архивирования журналов, хранящихся в базе данных сервера безопасности;
- "Почтовая рассылка о тревогах" — содержит параметры рассылки почтовых уведомлений при регистрации событий тревоги на подчиненных компьютерах;
- "Привилегии пользователей" — содержит список учетных записей с привилегиями для работы с Центром управления;
- "Фильтр тревог от подчиненных серверов" — содержит параметры фильтрации уведомлений о событиях тревоги, поступающих от серверов безопасности, которые подчинены выбранному серверу безопасности;
- "Аутентификация Windows" — содержит параметр, определяющий режим доверия аутентификации Windows в домене безопасности;

  Внимание! Параметр "Аутентификация Windows" является глобальным. При изменении значения данного параметра на одном сервере безопасности значение сменится на всех серверах внутри домена безопасности.

- "Управление трассировкой" — содержит параметры трассировки работы ПО системы Secret Net Studio (сервисная функция).

Набор параметров, доступных для просмотра и изменения, зависит от типа выбранного для управления объекта.

Параметры сетевых соединений

Управление параметрами сетевых соединений осуществляется в группе "Сетевые настройки". Группа присутствует при выборе сервера безопасности или защищаемого компьютера.

Параметры используются при установлении сетевого соединения объекта с сервером безопасности, которому подчинен данный объект. Для корневого СБ настройка данных параметров не требуется.

Сетевое взаимодействие компонентов системы Secret Net Studio дает определенную нагрузку на каналы связи. Устойчивость сетевых соединений и затрачиваемое время на передачу данных зависят от пропускной способности сети. Если пропускная способность низкая (например, при использовании модемного соединения), возможны длительные задержки при установлении соединений и даже сбои при передаче данных.

Чтобы обеспечить нормальное функционирование системы на медленных каналах связи, администратору безопасности следует проверить и при необходимости откорректировать параметры сетевого взаимодействия объектов. Данные параметры определяют интервалы времени ожидания при выполнении сетевых запросов.

Примечание. Снизить нагрузку на каналы связи можно и другими способами. Например, посредством изменения параметров синхронизации заданий контроля целостности, по умолчанию применяемых на компьютерах (см. документ [**2**]).

Для настройки параметров сетевых соединений:

1. В поле "Шаблоны сетевых настроек" выберите нужный шаблон для настройки параметров сетевого взаимодействия. Значения остальных полей изменяются автоматически в соответствии с выбранным шаблоном. При необходимости значения можно отредактировать вручную (описание параметров см. на стр.**282**).
2. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Параметры передачи локальных журналов

Управление параметрами передачи локальных журналов осуществляется в группе "Сбор журналов". Группа присутствует при выборе сервера безопасности или защищаемого компьютера.

Параметры сбора локальных журналов, заданные для сервера безопасности, относятся ко всем компьютерам, которые подчинены данному серверу. При этом на отдельных компьютерах можно настроить индивидуальные параметры, которые будут иметь более высокий приоритет по сравнению с заданными параметрами на сервере безопасности.

Содержимое локальных журналов защищаемых компьютеров должно своевременно поступать в централизованные журналы в базе данных сервера безопасности. Длительные перерывы в отправке могут привести к переполнению локальных журналов или к чрезмерной нагрузке на сервер безопасности и каналы связи при получении больших объемов данных.

Чтобы избежать проблем, связанных с несвоевременной передачей данных, администратору безопасности следует проверить и при необходимости откорректировать максимальный размер журнала системы защиты и условия перезаписи событий (настраивается в разделе "Базовая защита" для группы параметров "Журнал"), настроить параметры и расписание сбора журналов (настраивается в разделе "Параметры" для группы параметров "Сбор журналов"). Эти параметры задают условия для передачи локальных журналов на сервер безопасности и расписание запуска процесса передачи. Параметры следует настроить таким образом, чтобы, с одной стороны, минимизировать загруженность сетевых каналов в пиковые моменты времени (например, в начале рабочего дня или в запланированное время загрузки обновлений ПО на компьютерах) и, с другой стороны, не допустить переполнение журналов на защищаемых компьютерах (так как при переполнении локального журнала доступ пользователя к компьютеру может быть ограничен).

Для настройки параметров передачи журналов:

1. Настройте базовые параметры в группе полей "Производить сбор журналов":
   - если запуск процесса сбора журналов должен выполняться при каждом подключении компьютеров к серверу безопасности, установите отметку в поле "При подключении агента к серверу безопасности";

- если на сервер безопасности необходимо передавать журналы, близкие к переполнению, установите отметку в поле "При заполнении журнала на 80% и более".

  Пояснение. Система защиты контролирует заполнение локального журнала на компьютере и инициирует его передачу на сервер, когда текущий размер журнала достигнет 80% от заданного для него максимально допустимого размера. Передача осуществляется после получения подтверждения о готовности сервера безопасности. Во время пиковой загруженности сервера прием переполненного журнала откладывается.

2. При необходимости отключите централизованный сбор журналов определенных типов. Для этого удалите отметки в соответствующих полях группы "Включить в сбор следующие журналы". Централизованный сбор можно отключить только для штатных журналов ОС Windows, поэтому данная возможность недоступна при настройке параметров агентов на компьютерах с Secret Net LSP.
3. Если требуется оставлять на компьютерах копии содержимого локальных журналов после передачи на сервер безопасности, установите отметку в поле "Сохранять копии журналов на защищаемом компьютере".

   Пояснение. Копии содержимого локальных журналов сохраняются на компьютере в evt-файлах в каталоге %ProgramData%\Security Code\Secret Net Studio\Client\OmsAgentEvtCopy. Обработка и удаление этих файлов выполняется администратором.
   Функция создания копий журналов предусмотрена для упрощения диагностики возникающих проблем. В нормальном режиме работы данная функция должна быть отключена.

4. Если запуск процесса передачи локальных журналов подключенных компьютеров должен выполняться в определенные моменты времени, настройте расписание сбора журналов. Для этого выберите нужный режим в раскрывающемся списке поля "Расписание сбора журналов":

Периодическое
Запуск процесса передачи журналов осуществляется через равные промежутки времени. Продолжительность промежутка задается в минутах, часах или днях. Режим начинает действовать с момента наступления определенной даты и времени. Чтобы указать другой момент начала действия режима, выберите ссылку с текущим значением даты и времени и в появившемся на экране диалоге укажите нужные значения
Еженедельное
Запуск процесса передачи журналов осуществляется в моменты времени, заданные расписанием. Расписание представлено в виде таблицы. В столбцах таблицы перечислены дни недели, а в строках — часы. Выбор времени запуска процесса осуществляется посредством выделения соответствующей ячейки таблицы. Действие расписания повторяется еженедельно

   Чтобы отключить режим передачи журналов по расписанию, выберите в раскрывающемся списке значение "Не задано". Если режим отключен для защищаемого компьютера, будут применяться параметры расписания, заданные для родительского объекта. Чтобы перейти к этим параметрам, выберите ссылку "Перейти на действующее расписание родительского объекта".

   Примечание. Параметры расписания, заданные для сервера безопасности, не применяются на компьютерах с индивидуально настроенными расписаниями передачи журналов.

5. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Параметры сервера

Управление параметрами сервера осуществляется в группе "Конфигурация сервера". Группа присутствует при выборе сервера безопасности.

На сервере должен быть установлен сертификат для обеспечения возможности подчинения агентов. При наличии корректного сертификата в поле "Сертификат сервера" отображается ссылка "Установлен", позволяющая вызвать стандартное окно с подробными сведениями о сертификате сервера безопасности.

По умолчанию для размещения каталогов архива и временных файлов, создаваемых сервером безопасности, используются локальные папки в каталоге установки ПО сервера. При необходимости можно указать другие пути размещения файлов в поле "Расположение файлов на сервере" — для этого введите полный путь в соответствующем поле и нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Примечание. В случае использования сетевого пути необходимо на компьютере, где находится сетевой ресурс, стандартными средствами предоставить права доступа к папке для учетной записи компьютера сервера безопасности. При этом права доступа других учетных записей следует ограничить. Настройка прав доступа осуществляется в диалоговом окне настройки свойств папки на вкладках "Безопасность" (разрешения на доступ к папке) и "Доступ" (разрешения для общего ресурса). В списках учетных записей нужно добавить учетную запись компьютера сервера безопасности и при настройке разрешений на доступ к папке назначить разрешения "Чтение" и "Запись", а при настройке разрешений для общего ресурса — назначить разрешения "Чтение" и "Изменение".

Параметры архивирования централизованных журналов

Управление параметрами архивирования централизованных журналов осуществляется в группе "Архивирование журналов". Группа присутствует при выборе сервера безопасности.

Параметры задают расписание автоматического архивирования централизованных журналов. Архивирование применяется к записям журналов, которые поступили от подчиненных защищаемых компьютеров и хранятся в базе данных сервера безопасности.

С целью обеспечения сохранности информации следует проводить регулярное архивирование базы данных. В некоторых версиях СУБД действуют ограничения на объем баз данных. Если размер базы превысит ограничение, поступление новой информации будет невозможно до очистки БД.

Наряду с обеспечением сохранности информации архивирование дает возможность вывести из базы данных неактуальные сведения, чтобы сократить время выполнения запросов к БД. При необходимости просмотра старых записей о событиях в Центр управления можно загрузить файлы архивных копий.

Архивирование может выполняться по заданному расписанию для сервера безопасности или по специальной команде, доступной в Центре управления.

Для настройки параметров архивирования:

1. Выберите в раскрывающемся списке нужный режим:

Периодическое
Запуск процесса архивирования осуществляется через равные промежутки времени. Продолжительность промежутка задается в минутах, часах или днях. Режим начинает действовать с момента наступления заданной даты и времени. Чтобы указать другой момент начала действия режима, выберите ссылку с текущим значением даты и времени и в появившемся на экране диалоге укажите нужные значения
Еженедельное
Запуск процесса архивирования осуществляется в моменты времени, заданные расписанием. Расписание представлено в виде таблицы. В столбцах таблицы перечислены дни недели, а в строках — часы. Выбор времени запуска процесса осуществляется посредством выделения соответствующей ячейки таблицы. Действие расписания повторяется еженедельно

   Чтобы отключить режим автоматического запуска процесса архивирования, выберите в раскрывающемся списке значение "Не задано".

2. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Параметры рассылки уведомлений о событиях тревоги

Управление параметрами рассылки уведомлений о событиях тревоги осуществляется в группе "Почтовая рассылка о тревогах". Группа присутствует при выборе сервера безопасности.

При регистрации событий тревоги на защищаемых компьютерах, подчиненных серверу безопасности или его подчиненным серверам, система Secret Net Studio может автоматически оповещать об этом ответственных сотрудников. Оповещение осуществляется в виде уведомлений, рассылаемых по электронной почте.

Рассылка выполняется по специальным правилам, распределяющим уведомления в зависимости от источников регистрации, категорий или кодов событий. В соответствии с заданными правилами на сервере безопасности будет выполняться обработка всех зарегистрированных событий тревоги, сведения о которых были получены сервером.

Например, можно настроить рассылку уведомлений следующим образом:

- при возникновении событий тревоги категории "Вход/выход" уведомления направляются системному администратору;
- при возникновении события тревоги какой-либо категории уведомления направляются администратору безопасности и аудитору.

Для настройки параметров почтовой рассылки:

1. Сформируйте список правил рассылки уведомлений. Управление списком правил осуществляется с помощью кнопок, расположенных под списком.

Кнопка	Описание
Редактировать	Вызывает диалоговое окно для настройки параметров выбранного правила (см. ниже)
Добавить	Добавляет новое правило в список. Для нового правила выполняется настройка параметров в диалоговом окне (см. ниже)
Удалить	Удаляет выбранный элемент из списка

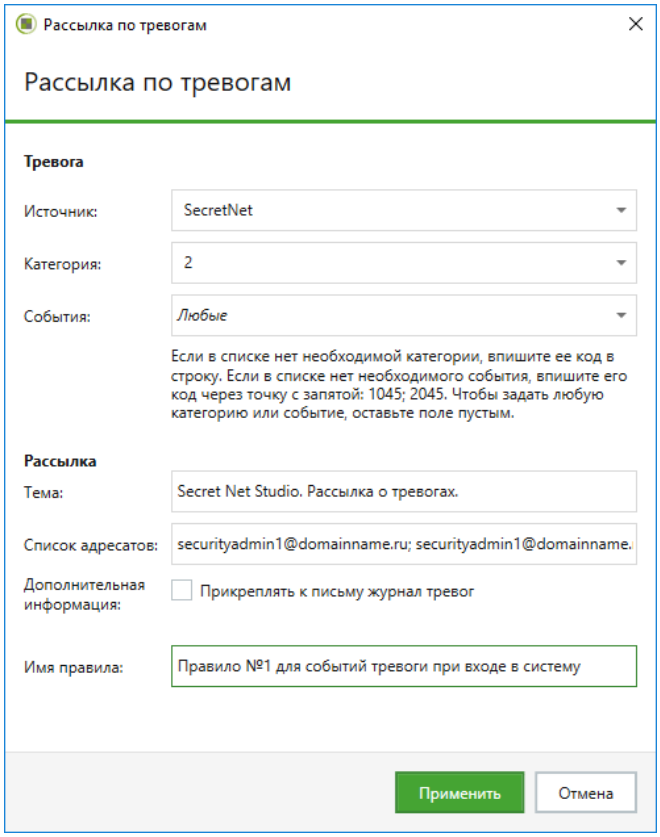
2. В поле "Почтовый сервер" введите имя или IP-адрес почтового сервера, через который будет выполняться рассылка уведомлений. В поле "Порт" укажите номер порта для доступа к серверу.
3. В поле "От кого" введите, если требуется, адрес электронной почты, на который получатели уведомлений смогут направлять ответные сообщения. Например, для этих целей может быть указан адрес электронной почты администратора безопасности.
4. При необходимости укажите учетные данные для доступа к почтовому серверу. Для этого установите отметку в поле "Использовать аутентификацию" и в появившемся окне введите имя и пароль пользователя.

Примечание.
- Параметр "Использовать аутентификацию" доступен для настройки только для сервера, к которому в данный момент подключен Центр управления.
- При необходимости изменения учетных данных для доступа к почтовому серверу нажмите кнопку "Сменить имя и пароль пользователя" и введите новые учетные данные.
- Для повышения защищенности рекомендуется в качестве пользователя, от лица которого будет рассылка, указывать отдельно выделенную гостевую учетную запись с минимальным набором привилегий в домене AD.

5. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Настройка параметров правила рассылки

Пример диалогового окна настройки параметров правила рассылки представлен на рисунке ниже.



Для настройки параметров правила рассылки:

1. В поле "Имя правила" отредактируйте имя для элемента в списке правил.
2. В группе полей "Тревога" настройте параметры анализа событий:

Источник
Содержит имя компонента или подсистемы, которое указывается при регистрации событий в качестве источника. Выберите нужный источник
Категория
Содержит числовой код категории событий. Выберите код нужной категории из раскрывающегося списка или введите значение вручную. Список категорий, доступных для выбора, формируется в зависимости от указанного источника
События
Содержит числовые идентификаторы событий. Выберите идентификаторы нужных событий из раскрывающегося списка или введите значение вручную. Список событий, доступных для выбора, формируется в зависимости от указанной категории. Несколько идентификаторов разделяются символом ";"

Примечание. Сведения о событиях можно получить при просмотре записей журнала событий тревоги на вкладке "Общее" (см. стр. 191). Источники, коды категорий и идентификаторы событий представлены, соответственно, в следующих полях вкладки: "Источник", "Код категории" и "Событие".

3. В группе полей "Рассылка" настройте параметры рассылки уведомлений:

Тема
Содержит строку, которая будет указываться в уведомлениях в качестве темы электронного сообщения
Список адресатов
Содержит список электронных адресов получателей уведомлений. Несколько адресов разделяются символом ";"

Дополнительная информация
Если поле содержит отметку, уведомления будут содержать дополнительные сведения о событиях тревоги (в виде прикрепленных к письмам текстовых файлов). Действие параметра распространяется только на компьютеры, подчиненные данному серверу безопасности. Сведения не добавляются в уведомления о событиях тревоги, произошедших на защищаемых компьютерах транзитивного подчинения (относящихся к подчиненным серверам)

4. Нажмите кнопку "Применить".

Привилегии для работы с Центром управления

Управление привилегиями пользователей для работы с Центром управления осуществляется в группе параметров "Привилегии пользователей" настроек сервера безопасности.

Пользователям и группам пользователей могут быть назначены следующие привилегии:

- "Просмотр информации" — привилегия для подключения к серверу безопасности и просмотра информации, построения отчетов;
- "Редактирование иерархии и параметров объектов" — привилегия для редактирования конфигурации объектов и управления параметрами в разделе "Параметры";
- "Выполнение оперативных команд" — привилегия на выполнение команд оперативного управления;
- "Редактирование политик" — привилегия для управления параметрами в разделах "Политики" и "Регистрация событий";
- "Квитирование сообщений о тревогах" — привилегия на выполнение команд квитирования событий тревоги;
- "Сбор журналов по команде" — привилегия на выполнение внеочередной передачи локальных журналов компьютеров;
- "Архивирование/восстановление журналов" — привилегия на выполнение процедур архивирования или восстановления централизованных журналов;
- "Загрузка СПС из файла" — привилегия на выполнение команды загрузки в базу сервера безопасности собранных сведений о состоянии программной среды компьютера;
- "Утверждение паспорта ПО" — привилегия на выполнение команды утверждения проекта паспорта в качестве текущего паспорта компьютера;
- "Синхронизация базы данных паспортов ПО" — привилегия на выполнение команды синхронизации сведений о паспортах, расположенных на сервере безопасности;
- "Удаление паспорта ПО" — привилегия на выполнение команды удаления паспортов, кроме текущего утвержденного паспорта;
- "Администрирование системы защиты" — привилегия для управления параметрами механизма самозащиты.

По умолчанию все перечисленные привилегии предоставлены пользователям, входящим в группу администраторов домена безопасности. При необходимости привилегии можно назначить и другим учетным записям, исключая привилегию "Редактирование иерархии и параметров объектов" — данная привилегия в обязательном порядке предоставляется только для группы администраторов домена безопасности.

Для предоставления привилегий:

1. Сформируйте список пользователей и групп, которым необходимо предоставить привилегии. Для добавления и удаления учетных записей используйте кнопки под списком.

2. Предоставьте необходимые привилегии учетным записям. Для предоставления привилегии выберите учетную запись и установите отметку рядом с названием привилегии. Удаление отметки отменяет предоставление привилегии.

Особенности предоставления привилегий:
- Привилегия "Просмотр информации" назначается автоматически для всех учетных записей, представленных в списке "Пользователи и группы".
- Привилегия "Редактирование иерархии и параметров объектов" не может быть предоставлена добавленным учетным записям.
- Чтобы редактировать параметры группы защиты сетевых подключений в разделе "Политики", пользователю должны быть предоставлены привилегии "Редактирование политик" и "Редактирование иерархии и параметров объектов". В связи с этим редактирование указанных параметров доступно только для пользователей группы администраторов домена безопасности.

3. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Параметры фильтра уведомлений о событиях тревоги на подчиненных СБ

В группе "Фильтр тревог от подчиненных серверов" осуществляется управление фильтрацией событий тревоги для ограничения поступающих уведомлений от защищаемых компьютеров следующих уровней подчинения (подчиненных серверов безопасности). Группа присутствует при выборе сервера безопасности.

За счет использования фильтра можно сократить сетевой трафик и обеспечить поступление уведомлений только о важных для администратора событиях.

Примечание. При настройке параметров политик (см. стр.145) можно задать параметр "Фильтр тревог" в группе "Оповещение о тревогах". Этот параметр ограничивает передачу уведомлений непосредственно на защищаемых компьютерах. Таким образом, средства управления фильтрацией событий тревоги можно использовать отдельно для защищаемых компьютеров и серверов. Это позволяет, например, задать разные параметры фильтрации для компьютеров, подчиненных серверу безопасности нижнего уровня (в разделе "Политики"), и для сервера верхнего уровня (в разделе "Параметры"). В этих условиях на сервере нижнего уровня уведомления о событиях тревоги на компьютерах будут отфильтрованы по одним критериям, а на сервере верхнего уровня события от тех же компьютеров — по другим критериям. В Центре управления количество поступающих уведомлений будет зависеть от того, к какому серверу выполнено подключение.

Ниже рассматривается процедура настройки фильтрации уведомлений в группе "Фильтр тревог от подчиненных серверов" раздела "Параметры". Настройка фильтрации в разделе "Политики" (группа "Оповещение о тревогах") осуществляется аналогично.

Фильтрация выполняется по списку правил. В правилах указываются условия для содержимого полей в записях журналов.

Список правил можно формировать при работе в группе "Фильтр тревог от подчиненных серверов" или с помощью средств панели событий системы (см. стр.178).

Для настройки фильтрации событий тревоги:

1. Выберите режим функционирования фильтра. Для этого установите отметку в нужном поле:
   - "Не пропускать на сервер события из правил" — фильтр не пропускает уведомления о событиях тревоги, которые удовлетворяют условиям в правилах фильтрации;
   - "Пропускать на сервер только события из правил" — инверсный режим, при котором фильтр пропускает уведомления только о событиях тревоги, соответствующих правилам из списка.

Внимание! Не включайте инверсный режим при пустом списке правил. Иначе фильтр не будет пропускать все события тревоги. Режим "Пропускать на сервер только события из правил" целесообразно использовать, если требуется пропускать поступающие уведомления об определенных событиях, а остальные — блокировать. Для этого необходимо создать правила, описывающие такие события.

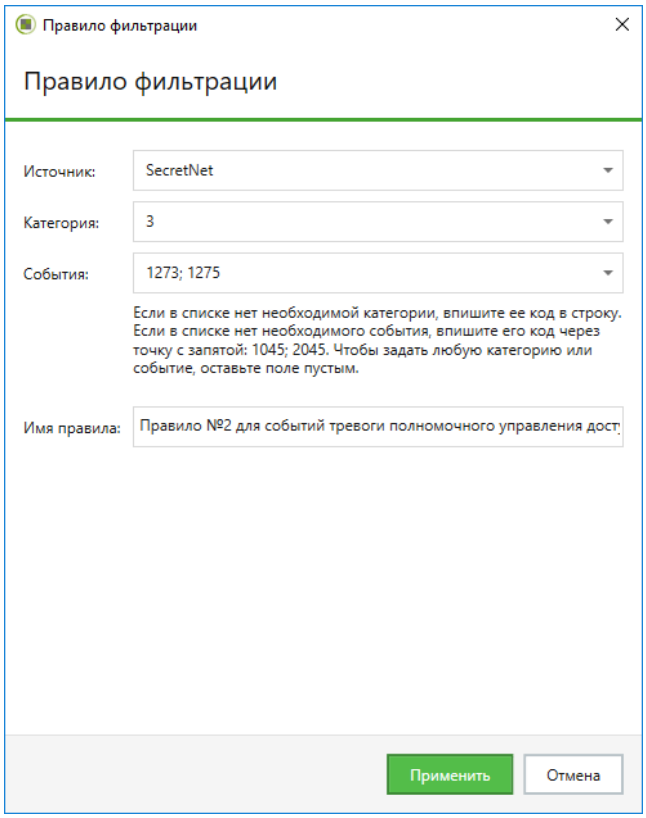
2. Сформируйте список правил фильтрации. Управление списком правил осуществляется с помощью кнопок, расположенных под списком.

Кнопка	Описание
Редактировать	Вызывает диалоговое окно для настройки параметров выбранного правила (см. ниже)
Добавить	Добавляет новое правило в список. Для нового правила выполняется настройка параметров в диалоговом окне (см. ниже)
Удалить	Удаляет выбранный элемент из списка

3. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Настройка параметров правила фильтрации

Пример диалогового окна настройки параметров правила фильтрации представлен на рисунке ниже.



Для настройки параметров правила фильтрации:

1. В поле "Имя правила" отредактируйте имя для элемента в списке правил.
2. Настройте параметры анализа событий.

Источник
Содержит имя компонента или подсистемы, которое указывается при регистрации событий в качестве источника. Выберите нужный источник
Категория

Содержит числовой код категории событий. Выберите код нужной категории из раскрывающегося списка или введите значение вручную. Список категорий, доступных для выбора, формируется в зависимости от указанного источника
События
Содержит числовые идентификаторы событий. Выберите идентификаторы нужных событий из раскрывающегося списка или введите значение вручную. Список событий, доступных для выбора, формируется в зависимости от указанной категории. Несколько идентификаторов разделяются символом ";"

Примечание. Сведения о событиях можно получить при просмотре записей журнала событий тревоги на вкладке "Общее" (см. стр. 191). Источники, коды категорий и идентификаторы событий представлены, соответственно, в следующих полях вкладки: "Источник", "Код категории" и "Событие".

3. Нажмите кнопку "Применить".

Параметры трассировки ПО системы Secret Net Studio

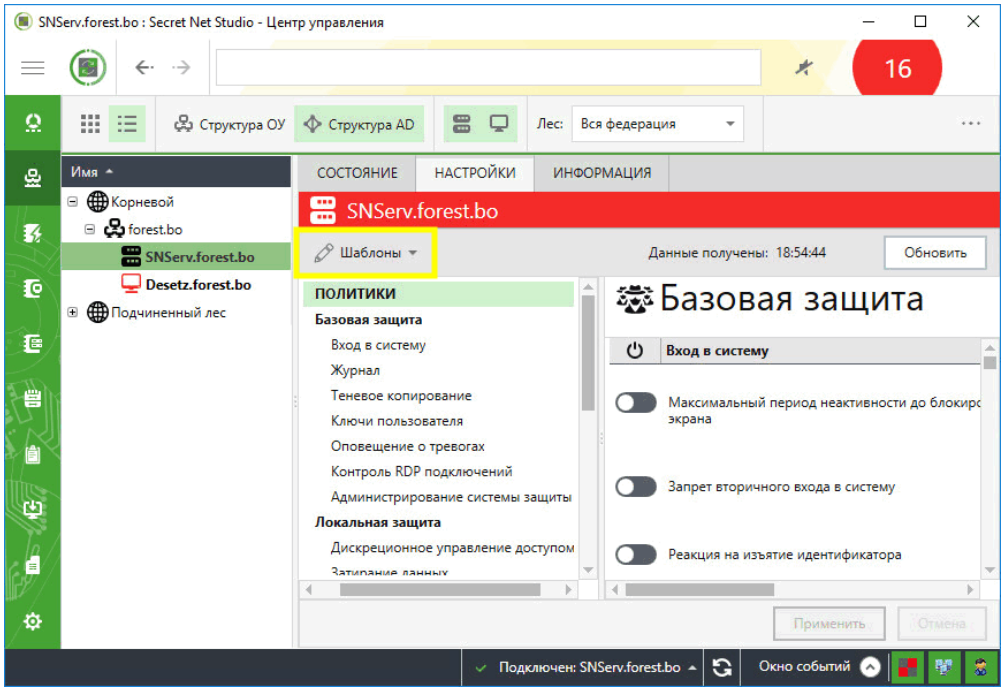
Центр управления предоставляет возможность централизованного включения и настройки параметров трассировки — сервисной функции для сбора информации о работе системы Secret Net Studio. При трассировке осуществляется запись в специальные файлы служебных данных о функционировании программных модулей. Эти данные необходимы для диагностики возникновения сбойных или ошибочных ситуаций.

Параметры трассировки входят в группу "Управление трассировкой", которая доступна при выборе сервера безопасности или компьютера под управлением ОС Windows. Сведения о необходимых действиях для настройки предоставляются при обращении в отдел технической поддержки компании "Код Безопасности".

Внимание! Не рекомендуется без необходимости включать функцию трассировки. В штатном режиме эксплуатации системы Secret Net Studio данная функция должна быть отключена, чтобы не создавать лишнюю нагрузку для компьютера.

Шаблоны параметров безопасности

Меню "Шаблоны" находится в панели "Компьютеры" на вкладке "Настройки".



Пояснение. Меню "Шаблоны" появится после загрузки параметров безопасности выбранного объекта с сервера безопасности. Для загрузки параметров в области отображения параметров нажмите кнопку "Загрузить настройки".

Меню "Шаблоны" содержит следующие пункты:

- "Создать по настройкам объекта управления" — создание шаблона с параметрами безопасности настроенного объекта (см. стр.**159**);
- "Применить" — применение параметров безопасности из существующих шаблонов (см. ниже);
- "Сравнить с" — сравнение параметров безопасности объекта с параметрами безопасности шаблона (см. стр.**160**).

Примечание.

- Шаблоны можно применить к группе однотипных объектов (к клиентам под управлением одной ОС, подчиненным одному и тому же серверу безопасности; к серверам безопасности под управлением одной ОС, находящимся в одном домене безопасности).
- Для применения и сравнения шаблонов пользователю необходимы права на редактирование политик.
- Для клиентов в сетевом режиме работы в Локальном центре управления недоступны настройка и применение политик сетевой защиты.

Применение

В Secret Net Studio – С можно применить следующие шаблоны:

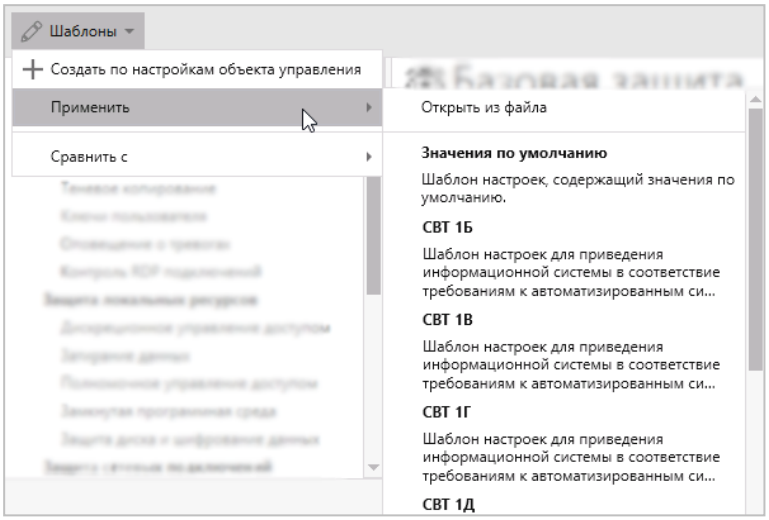
- стандартные шаблоны для приведения информационной системы в соответствие требованиям о защите информации для автоматизированных систем, государственных информационных систем и информационных систем персональных данных (см. стр.**224**);
- шаблон параметров безопасности, настроенных по умолчанию;
- шаблоны, созданные самостоятельно в Secret Net Studio (см. стр.**159**).

Примечание. Для компьютеров с Secret Net LSP можно применить только шаблоны, созданные самостоятельно.

Для применения шаблона:

1. Выберите в списке один или несколько компьютеров, вызовите для них панель свойств, перейдите на вкладку "Настройки" и нажмите кнопку "Загрузить настройки".
2. В меню "Шаблоны" выберите пункт "Применить".

   Появится перечень шаблонов:

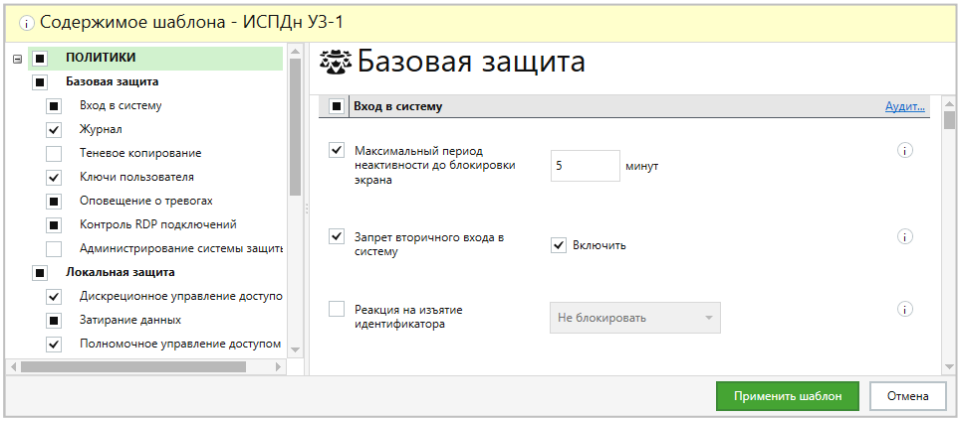


3. В перечне выберите шаблон, который необходимо применить:
   - "Открыть из файла" — для применения ранее созданного шаблона;

     Примечание. При выборе данного пункта откроется стандартный диалог ОС для открытия файла. Выберите шаблон параметров безопасности, который хотите применить, и нажмите "Открыть".

   - "Значения по умолчанию" — для применения шаблона параметров безопасности, настроенных по умолчанию;
   - "СВТ 1Б", "СВТ 1В" и др. — для применения шаблона, содержащего параметры безопасности для информационной системы определенного типа и класса/уровня защиты.

   Появится окно с содержимым шаблона.



   Совет. Для просмотра справочной информации о шаблоне нажмите кнопку  .

4. Проверьте значения параметров на соответствие требованиям о защите информации, предъявляемым к информационной системе. Используйте область оглавления для выбора группы параметров и область отображения параметров для просмотра значений параметров выбранной группы.

Пояснение. Группы параметров и параметры обозначаются пиктограммой в зависимости от их наличия или отсутствия в шаблоне:

- ☐ — отсутствует;
- ■ — частично имеется (только для группы параметров; означает, что не все параметры группы включены в шаблон);
- ☑ — имеется.

Если вы не хотите применять группу параметров или параметр шаблона, установите соответствующую пиктограмму в значение "отсутствует". В этом случае при применении шаблона группа параметров или параметр не изменит свое значение.

5. Нажмите кнопку "Применить шаблон".

Совет. Для отмены действия нажмите "Отмена".

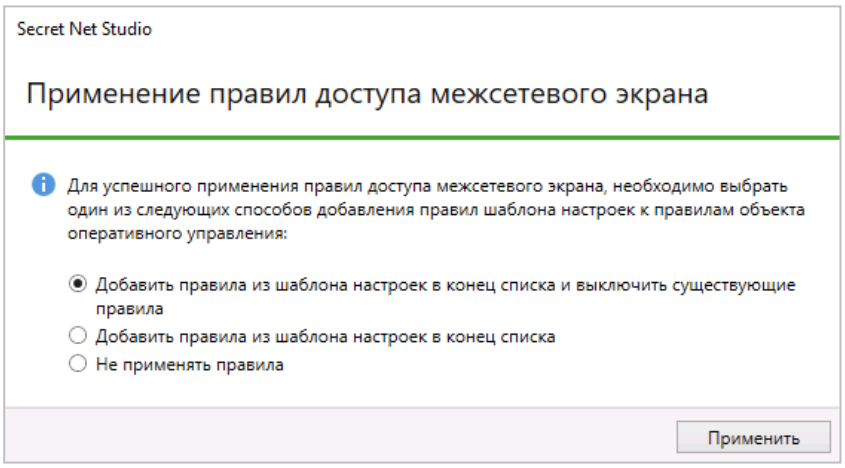
Система выдаст запрос на подтверждение действия.

6. Нажмите "Да".

Совет. Для отмены действия нажмите "Нет".
Для возврата к просмотру и корректировке параметров нажмите "Отмена".

Далее возможна следующая реакция системы.

- При применении шаблона с правилами МЭ к клиенту или группе клиентов система выдаст диалоговое окно для выбора способа применения правил МЭ шаблона к объекту.



  Выберите нужный способ добавления настроек и нажмите "Применить".

- При применении шаблона к группе клиентов с групповыми политиками система выдаст сообщение о наличии на клиенте групповых политик. В этом случае при применении шаблона групповые политики не изменяются.

7. Ожидайте, пока система применит шаблон параметров безопасности.

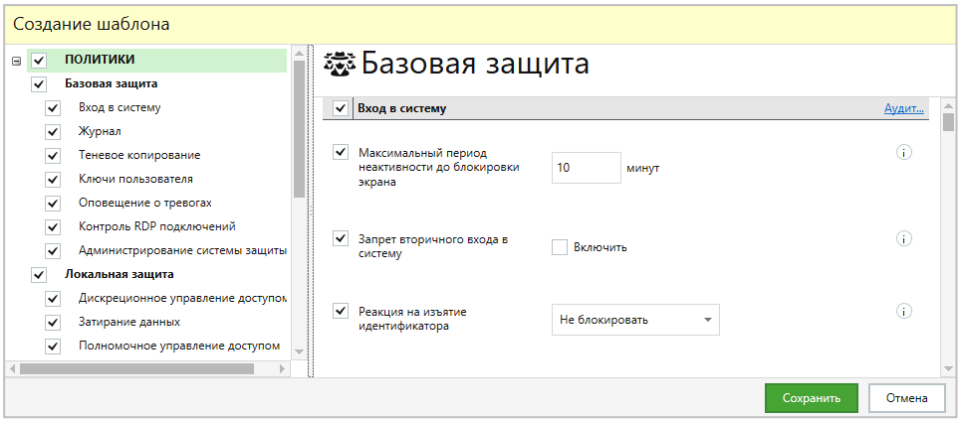
Создание

В Secret Net Studio настройки параметров безопасности объекта можно сохранить в шаблон для дальнейшего применения этого шаблона на других компьютерах.

Для создания шаблона:

1. Выберите в списке нужный компьютер, вызовите для него панель свойств, перейдите на вкладку "Настройки" и нажмите кнопку "Загрузить настройки".
2. В меню "Шаблоны" выберите пункт "Создать по настройкам объекта управления".

   Окно примет вид:



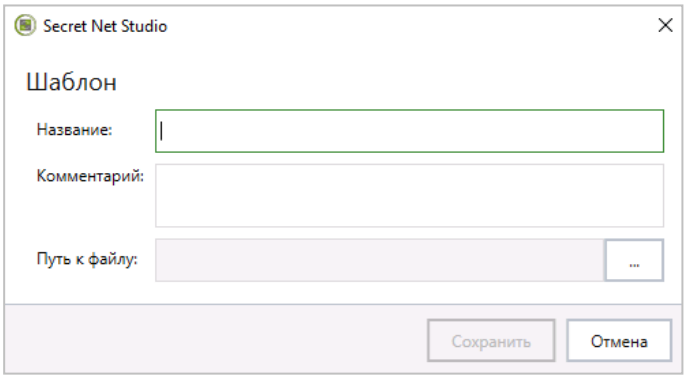
Пояснение. Группы параметров и параметры обозначаются пиктограммой в зависимости от их наличия или отсутствия в шаблоне:

- ☐ — отсутствует;
- ■ — частично имеется (только для группы параметров; означает, что не все параметры группы включены в шаблон);
- ☑ — имеется.

По умолчанию при создании шаблона в него включаются все параметры.

3. При необходимости измените значения параметров или исключите из шаблона группу параметров или параметр, установив соответствующую пиктограмму в значение "отсутствует".
4. Нажмите кнопку "Сохранить".

   Появится диалоговое окно для ввода информации о шаблоне:



5. Введите наименование шаблона, комментарий со справочной информацией о шаблоне и выберите путь к файлу, в который будет сохранен шаблон.

Совет. Для выбора пути к файлу нажмите кнопку ... . Появится стандартный диалог ОС для сохранения файла. Введите имя файла, укажите место сохранения файла и нажмите "Сохранить".

6. Нажмите кнопку "Сохранить".

   Шаблон будет сохранен в файле с расширением .omstemplate.

Сравнение

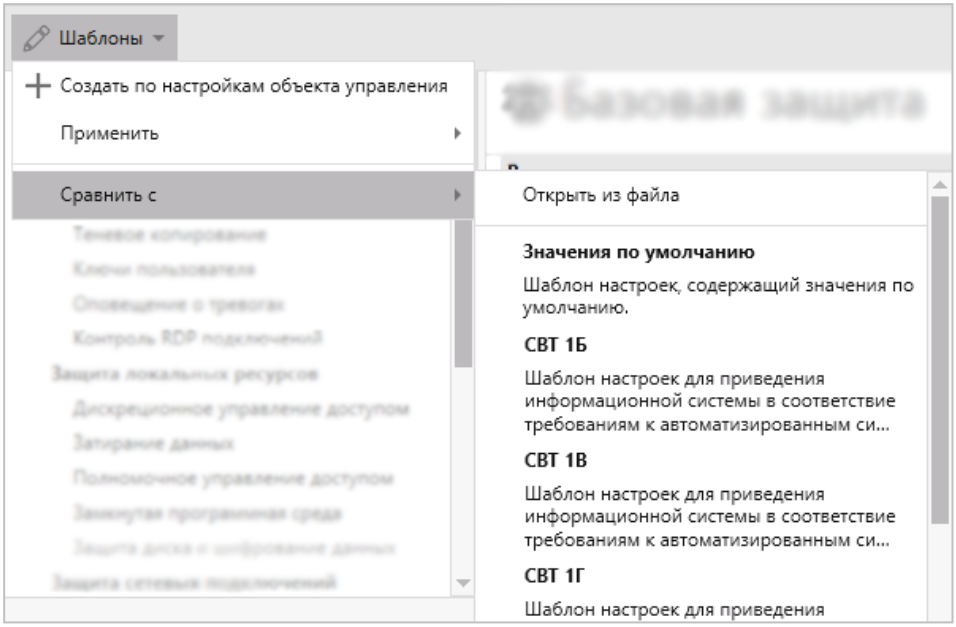
В Secret Net Studio имеется возможность сравнения параметров безопасности объекта с параметрами безопасности шаблона, чтобы оценить степень соответствия настроек требованиям о защите информации.

Примечание. Для компьютеров с Secret Net LSP сравнение параметров безопасности можно выполнять только с шаблонами, созданными самостоятельно.

Для сравнения параметров безопасности объекта с шаблоном:

1. Выберите в списке нужный компьютер, вызовите для него панель свойств, перейдите на вкладку "Настройки" и нажмите кнопку "Загрузить настройки".
2. В меню "Шаблоны" выберите пункт "Сравнить с".

   Появится перечень шаблонов.

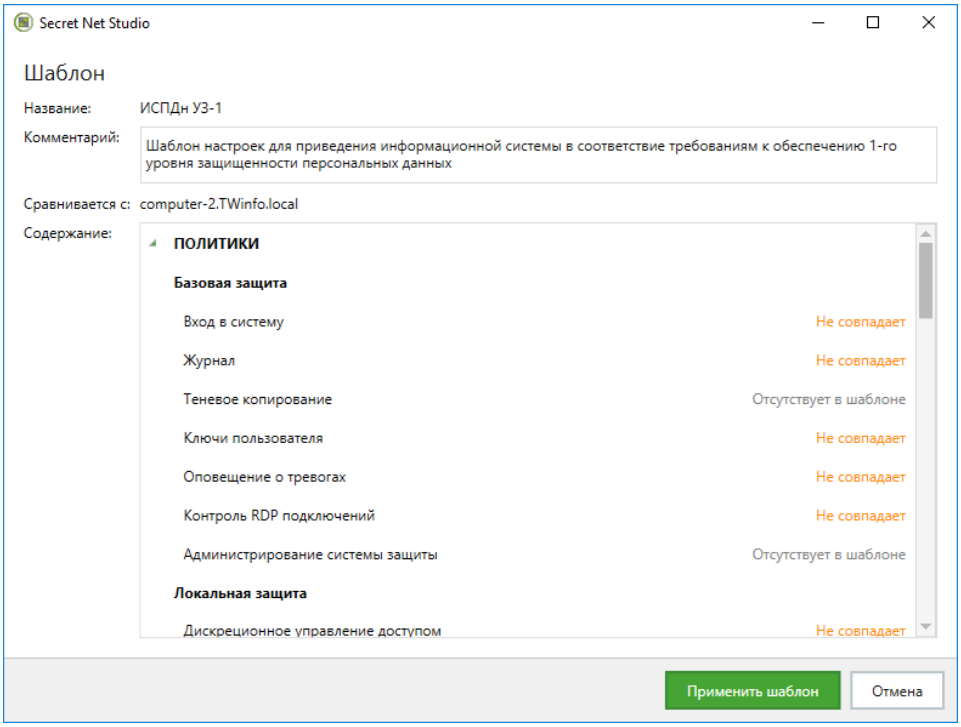


3. В перечне выберите шаблон, с которым нужно сравнить параметры безопасности объекта:
   - "Открыть из файла" — для выбора ранее созданного шаблона;

     Примечание. При выборе данного пункта откроется стандартный диалог ОС для открытия файла. Выберите шаблон, с которым хотите сравнить параметры безопасности объекта, и нажмите "Открыть".

   - "Значения по умолчанию" — для выбора шаблона параметров безопасности, настроенных по умолчанию;
   - "СВТ 1Б", "СВТ 1В" и др. — для выбора шаблона, содержащего параметры безопасности для информационной системы конкретного типа и класса/уровня защиты.

   Появится окно с результатом сравнения.



Пояснение. Возможны следующие результаты сравнения параметров:

- "Совпадает" — параметр шаблона совпадает с параметром объекта;
- "Не совпадает" — параметр шаблона не совпадает с параметром объекта;
- "Отсутствует" — параметр отсутствует в шаблоне;
- "Не поддерживается" — параметр имеется в шаблоне, но не поддерживается объектом.

4. Изучите результаты сравнения.

Внимание! Если вы применили шаблон, а затем сравниваете примененные настройки с тем же шаблоном, могут не совпадать правила МЭ (Политики → Сетевая защита → Персональный межсетевой экран). Старые правила МЭ не удаляются при применении шаблона. Для совпадения необходимо настроить правила МЭ вручную.

5. Выберите дальнейшее действие:

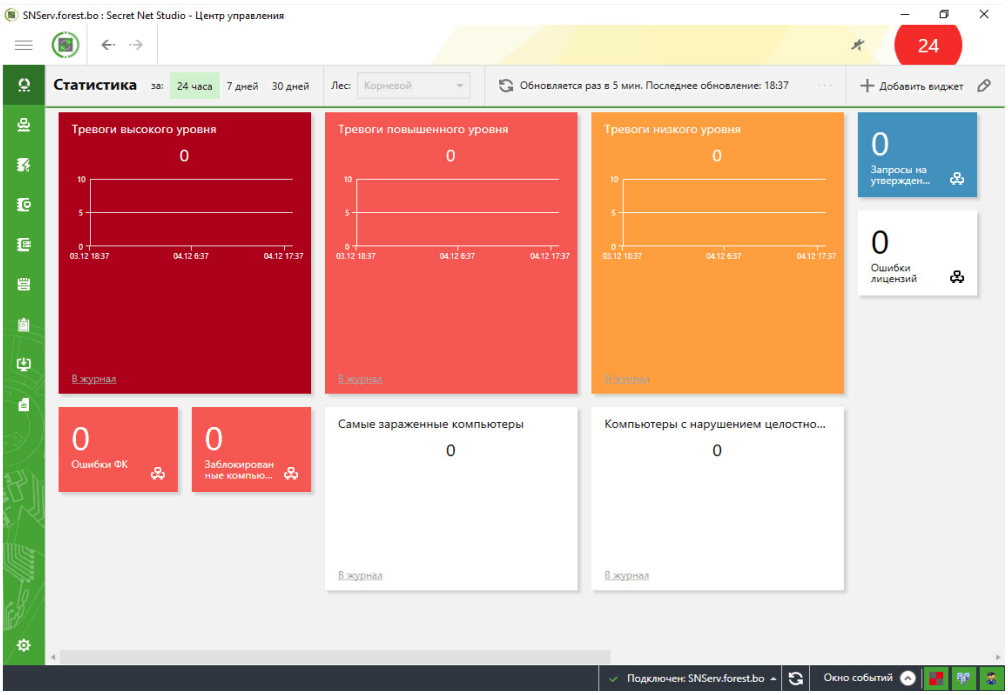
- для применения шаблона параметров безопасности, с которым выполнено сравнение, нажмите кнопку "Применить шаблон";
- для возврата к настройке параметров безопасности объекта нажмите кнопку "Отмена".

Глава 15
Мониторинг и оперативное управление

Общее состояние системы

Общие сведения

Сведения об общем состоянии защищенности системы содержатся в информационной панели "Статистика", пример которой представлен на следующем рисунке. Для просмотра этих сведений нажмите кнопку "Статистика" вверху панели навигации (слева в основном окне).



Информационная панель "Статистика" состоит из виджетов. Виджетом является визуальный элемент интерфейса программы, наглядно характеризующий один системный параметр. Панель виджета состоит из следующих элементов:

Элемент	Описание
Название	Наименование виджета
Состав	Может содержать следующую информацию: • показатель – число актуальных событий. Число является гиперссылкой, нажатие на которую позволяет посмотреть информацию о данных событиях в соответствующем журнале; • график – графическая форма распределения на интервале времени зарегистрированных событий. Столбик на графике является гиперссылкой, нажатие на которую позволяет посмотреть информацию о событии в соответствующем журнале; • список – перечень имен защищаемых компьютеров. Имя является гиперссылкой, нажатие на которую позволяет посмотреть информацию о защищаемом компьютере
Фон	Цвет панели виджета
В журнал	Является гиперссылкой на все зарегистрированные в соответствующем журнале события, связанные с данным системным параметром и всеми контролируемыми объектами

Наличие специальной пиктограммы на панели виджета свидетельствует об отображении данных обо всех компьютерах, подчиненных серверу безопасности, включая компьютеры, подчиненные его дочерним серверам.

Панель "Статистика" по умолчанию содержит фиксированный набор виджетов с настроенными параметрами, список которых представлен в следующей таблице.

Название	Фон	Состав
Тревоги высокого уровня	Бордовый	Показатель, график, список
Тревоги повышенного уровня	Красный	Показатель, график, список
Тревоги низкого уровня	Оранжевый	Показатель, график, список
Запросы на утверждение АК	Синий	Показатель
Ошибки лицензий	Белый	Показатель
Ошибки ФК	Красный	Показатель
Заблокированные компьютеры	Красный	Показатель
Самые зараженные компьютеры	Белый	Показатель, график, список
Компьютеры с нарушением целостности	Белый	Показатель, график, список

Полный перечень виджетов с их описанием представлен в следующей таблице.

Название	Описание	Состав
Базовая защита		
Топ компьютеров с запретами входа	Компьютеры с наибольшим количеством зарегистрированных событий запрета входа в систему	Список
Топ пользователей с запретами входа	Пользователи с наибольшим количеством зарегистрированных событий запрета входа в систему	Список
Тревоги высокого уровня	Число неквитированных тревог высокого уровня	Показатель, график, список
Тревоги повышенного уровня	Число неквитированных тревог повышенного уровня	Показатель, график, список
Тревоги низкого уровня	Число неквитированных тревог низкого уровня	Показатель, график, список
Ошибки ФК	Количество компьютеров с ошибками выполнения функционального контроля	Показатель
Запросы на утверждение АК	Количество компьютеров с запросом на утверждение аппаратной конфигурации	Показатель
Заблокированные компьютеры	Количество компьютеров, заблокированных системой защиты	Показатель
Топ компьютеров с нарушениями целостности	Компьютеры с наибольшим количеством зарегистрированных событий нарушения целостности при обработке заданий	Показатель, график, список
Локальная защита		
Топ компьютеров с запретами подключения устройств	Компьютеры с наибольшим количеством зарегистрированных событий запрета подключения устройств	Показатель, график, список
Топ компьютеров с запретами печати	Компьютеры с наибольшим количеством зарегистрированных событий запрета печати	Показатель, график, список

Название	Описание	Состав
Топ пользователей с запретами печати	Пользователи с наибольшим количеством зарегистрированных событий запрета печати	Показатель, график, список
Топ компьютеров с сетевыми атаками	Компьютеры с наибольшим количеством зарегистрированных событий об обнаруженных сигнатурах СОВ	Показатель, график, список
Топ атакующих узлов	Список наиболее часто встречающихся атакующих узлов в зарегистрированных событиях об обнаружении сигнатур СОВ	Список
Самые зараженные компьютеры	Компьютеры с наибольшим количеством зарегистрированных событий об обнаружении вируса	Показатель, график, список
Топ вирусов	Список наиболее часто встречающихся вирусов в зарегистрированных событиях об обнаружении вируса	Список
Топ компьютеров с вирусами в карантине	Список компьютеров с наибольшим числом вирусов в карантине	Список
Дополнительные виджеты		
Свободного места в БД	Процент свободного места в БД сервера подключения. Для MS SQL Server (полная версия) отображается свободное место файла БД без учета стратегии динамического увеличения	Показатель
Переполнение журнала	Количество компьютеров с событиями о переполнении журнала	Показатель
Ошибки лицензий	Количество компьютеров с нарушением лицензионной политики или истекшими лицензиями	Показатель

Примечание. При добавлении нового виджета на панель "Статистика" фон виджета по умолчанию является белым.

Редактирование параметров виджета

В виджете можно редактировать следующие параметры:

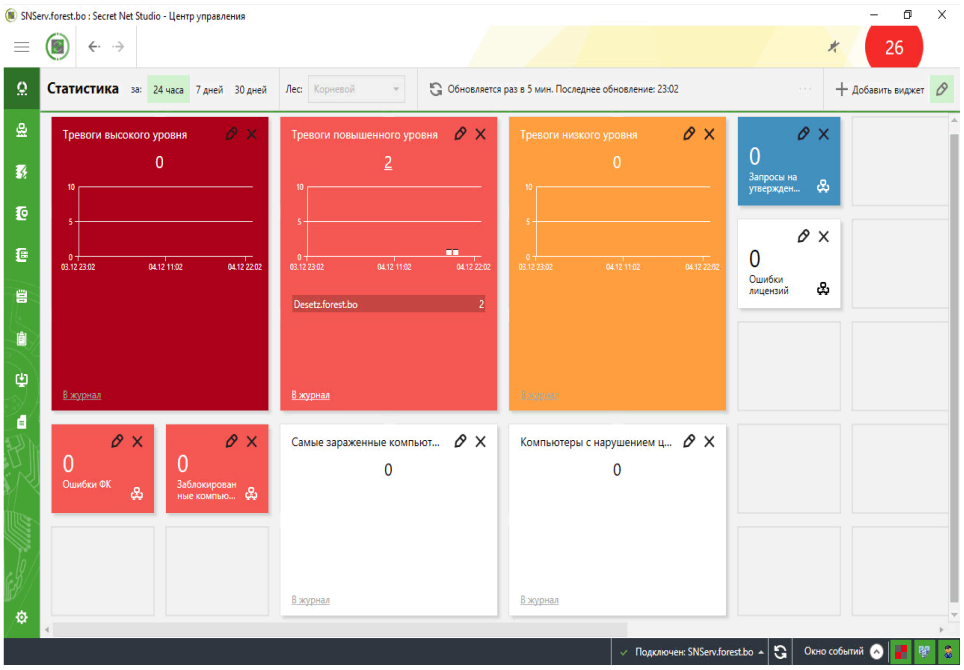
- название;
- состав;
- фон.

Процедура редактирования виджета выполняется в специальном диалоге.

Для вызова диалога редактирования виджета:

1. В правом верхнем углу панели нажмите кнопку "Редактировать виджеты".

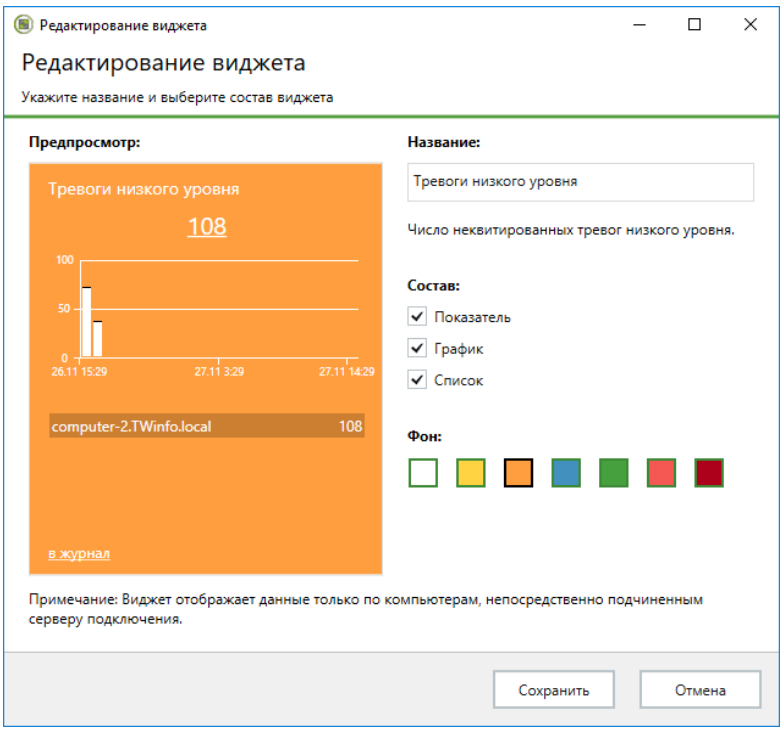
   В панели "Статистика" на панели каждого виджета появятся активные пиктограммы редактирования. Кнопка "Редактировать виджеты" изменит свой цвет на зеленый и появятся свободные ячейки для размещения виджетов.



Совет. При необходимости можно удалить любой виджет с информационной панели "Статистика", нажав пиктограмму "Удалить" на панели виджета.

2. На панели нужного виджета нажмите пиктограмму "Редактировать".

   На экране появится диалог, подобный следующему.



3. Измените параметры виджета и нажмите кнопку "Сохранить":
   - в поле "Название" укажите новое наименование виджета;
   - в поле "Состав" отметьте дополнительные параметры, которые будут отображены в виджете;
   - в поле "Фон" выберите цвет панели виджета.
4. Нажмите повторно кнопку "Редактировать виджеты".

В панели "Статистика" на панели каждого виджета исчезнут активные пиктограммы. Кнопка "Редактировать виджеты" изменит свой цвет и исчезнут свободные ячейки для размещения виджетов.

Добавление и удаление виджетов

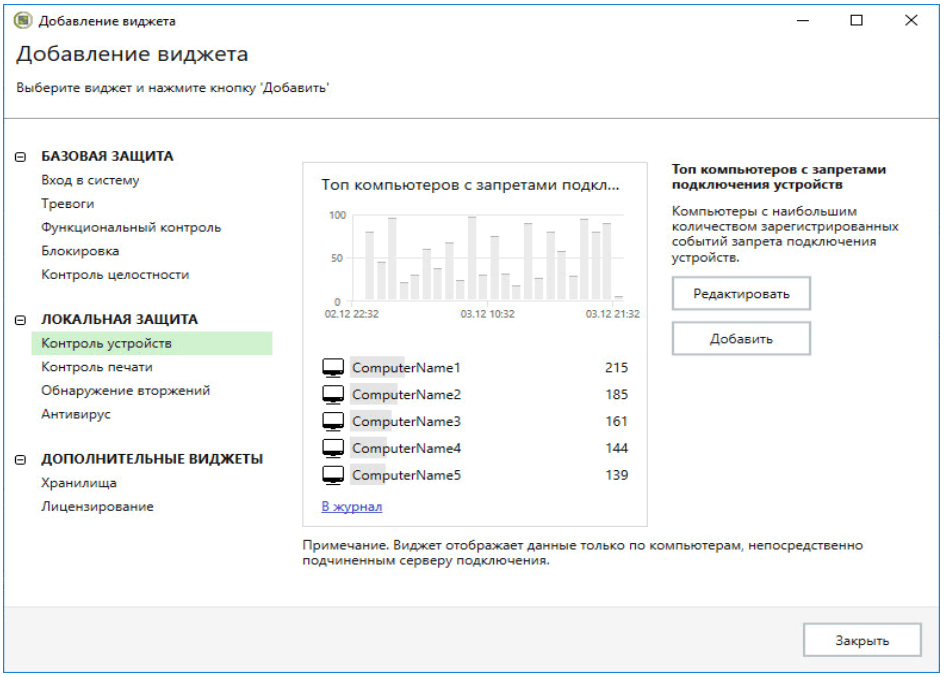
На панели "Статистика" можно добавлять и удалять виджеты.

Добавление виджетов

Для добавления виджетов:

1. В правом верхнем углу панели нажмите кнопку "Добавить виджет".

   На экране появится диалог добавления виджета.



2. В левой части диалога выберите в списке нужный виджет и нажмите кнопку "Добавить".

   Выбранный виджет добавится на панель "Статистика".

   Совет. При необходимости можно отредактировать доступные параметры выбранного виджета, нажав кнопку "Редактировать". Процедура редактирования виджета описана выше.

3. Для завершения работы с диалогом нажмите кнопку "Закрыть".

Удаление виджетов

Для удаления виджетов:

1. В правом верхнем углу панели нажмите кнопку "Редактировать виджеты".

   В панели "Статистика" на панели каждого виджета появятся активные пиктограммы редактирования. Кнопка "Редактировать виджеты" изменит свой цвет на зеленый и появятся свободные ячейки для размещения виджетов.

2. На панели нужного виджета нажмите пиктограмму "Удалить".

   Виджет исчезнет с панели "Статистика".

3. Нажмите повторно кнопку "Редактировать виджеты".

Перемещение виджетов

На панели "Статистика" можно перемещать виджеты.

Для перемещения виджетов:

1. В правом верхнем углу панели нажмите кнопку "Редактировать виджеты".

   В панели "Статистика" на панели каждого виджета появятся активные пиктограммы редактирования. Кнопка "Редактировать виджеты" изменит свой цвет на зеленый и появятся свободные ячейки для размещения виджетов.
2. Наведите указатель на панель виджета, нажмите и удерживайте нажатой левую кнопку мыши.
3. Переместите панель виджета в свободную ячейку и отпустите левую кнопку мыши.

   Виджет будет зафиксирован в новом положении.
4. Нажмите повторно кнопку "Редактировать виджеты".

Настройка временных параметров отображения данных

К данным параметрам панели "Статистика" относятся период, за который отображаются данные, и период обновления отображаемых данных.

Период, за который отображаются данные

Данный параметр может принимать одно из трех следующих значений:

- 24 часа;
- 7 дней;
- 30 дней.

Для настройки параметра:

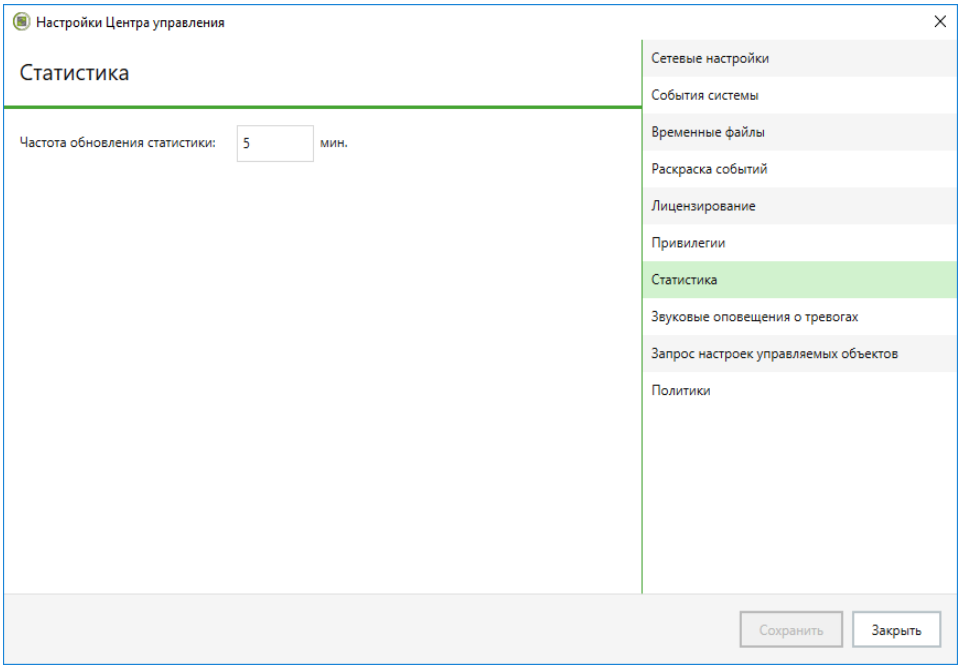
- В левом верхнем углу панели в группе "Статистика" нажмите кнопку с нужным значением периода времени, за который будут отображаться данные в панелях виджетов.

Период обновления данных

Вверху панели отображается значение интервала времени, определяющего периодичность автоматического обновления информации на панелях виджетов. Обновление может происходить как автоматически, так и принудительно при нажатии кнопки с информацией об обновлении. Период автоматического обновления данных можно изменить.

Для настройки периода обновления данных:

1. В нижней части панели навигации (слева в основном окне программы) нажмите кнопку "Настройки" и в появившейся панели выберите ссылку "Настройки Центра управления".
2. В появившемся диалоге выберите группу параметров "Статистика" и установите время в поле "Частота обновления статистики".



3. Нажмите кнопку "Сохранить" и закройте диалог.

Группы наблюдения

Группа наблюдения содержит информацию об общем состоянии уровня тревог в системе. Для оперативного мониторинга администратор может сформировать произвольные группы наблюдения, состоящие из компьютеров. Группа наблюдения является виджетом на панели "Статистика".

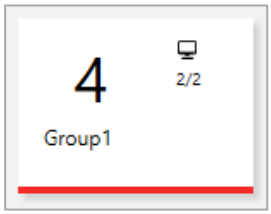


Рис.2 Пример виджета группы наблюдения

Панель виджета содержит в себе перечень отображаемых параметров:

- показатель — общее число тревог всех уровней по всем компьютерам группы наблюдения;

  Совет. При наведении курсора на показатель появляются данные о количестве тревог согласно их уровням. Отображается общее число компьютеров и число компьютеров с тревогами.

- наименование — название группы наблюдения;
- пиктограмма с изображением компьютера — число компьютеров с тревогами и число компьютеров в группе.

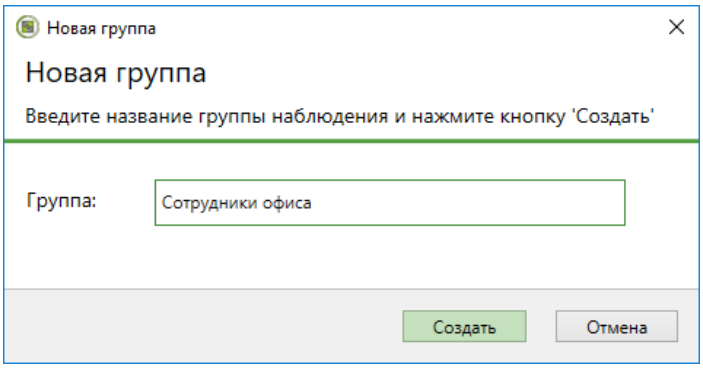
Контекстное меню виджета содержит следующие команды:

- "Перейти к компьютерам" — переход на панель "Компьютеры" к перечню компьютеров группы наблюдения;
- "Квитировать" — квитирование тревог на компьютерах группы наблюдения (всех имеющихся тревог или избирательно по выбранному уровню тревоги);
- "Журнал" — переход к журналу тревог с отображением выборки всех зарегистрированных на компьютерах группы тревог или избирательно по выбранному уровню тревоги;
- "Удалить группу..." — удаление группы наблюдения.

Для создания группы наблюдения:

1. В панели "Компьютеры" установите режим отображения списка компьютеров и выберите компьютеры, для которых нужно создать группу наблюдения.
2. Вызовите контекстное меню одного из выбранных компьютеров и выберите команду "Наблюдение | Новое...".

   Появится диалог "Новая группа".



3. В поле "Группа" укажите название группы наблюдения и нажмите кнопку "Создать".
4. После создания группы наблюдения перейдите на панель "Статистика".

   В панели "Статистика" появится созданный виджет.

Для добавления компьютеров в существующую группу наблюдения:

1. В панели "Компьютеры" установите режим отображения списка компьютеров и выберите компьютеры, которые нужно добавить в группу наблюдения.
2. Вызовите контекстное меню одного из выбранных компьютеров и выберите команду "Наблюдение | Добавить в... | <*Название группы*>".

Для удаления компьютеров из группы наблюдения:

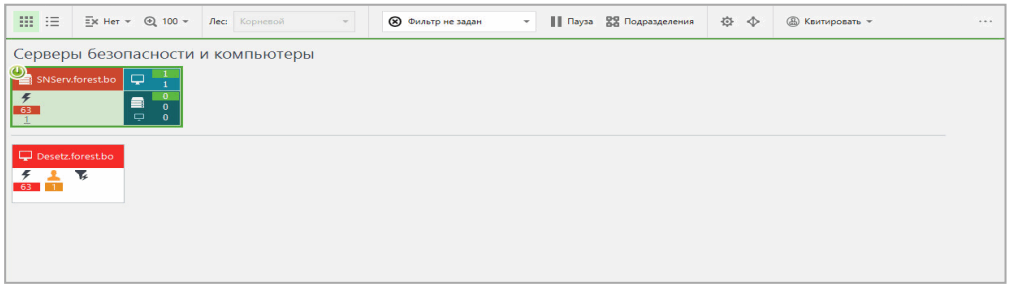
1. В панели "Компьютеры" установите режим отображения списка компьютеров и выберите компьютеры, которые нужно добавить в группу наблюдения.
2. Вызовите контекстное меню одного из выбранных компьютеров и выберите команду "Наблюдение | Удалить из... | <*Название группы*>".

Просмотр сведений

Обозначения объектов на диаграмме управления

Элементы диаграммы управления отображают основные сведения о состоянии объектов. Сведения представлены в виде пиктограмм и расположенных рядом числовых данных (например, количество событий тревоги на защищаемом компьютере или количество открытых сессий пользователей).

Пример диаграммы управления с отображаемыми сведениями представлен на рисунке ниже.



Сервер безопасности, с которым установлено соединение, обозначается специальной пиктограммой.

Для серверов безопасности и групп компьютеров числовые данные приводятся в двух или более строках: верхняя строка содержит общее количество событий/признаков на всех подчиненных компьютерах (например, сводное количество событий тревоги или количество включенных компьютеров), а нижние строки отображают количество компьютеров или подчиненных серверов безопасности с компьютерами. Некоторые числовые данные являются ссылками, которые можно использовать для фильтрации списков компьютеров. Например, чтобы отобразить в диаграмме только компьютеры с признаками тревоги.

Дополнительные сведения об объектах отображаются во всплывающих окнах, которые появляются при наведении указателя мыши на объекты.

Перечень предусмотренных пиктограмм представлен в следующей таблице:

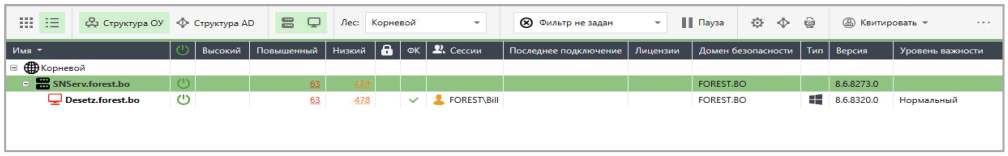
Пиктограмма	Описание
	Включена блокировка компьютера (компьютеров). Число соответствует количеству причин блокировки. В приведенном примере — одна причина
	На компьютере (компьютерах) зафиксированы события тревоги. Число является счетчиком зарегистрированных событий наивысшего уровня тревоги. Максимальное числовое значение счетчика — 999 событий. В случае превышения ограничения счетчик отображает значение "99+"
	На компьютере (компьютерах) зафиксированы ошибки (красный цвет пиктограммы) или предупреждения (желтый цвет) при проверке лицензий на использование компонентов системы Secret Net Studio. Число является счетчиком включенных подсистем с ошибкой лицензии
	На компьютере (компьютерах) зафиксировано изменение аппаратной конфигурации
	На компьютере (компьютерах) открыты сессии работы пользователей. Число соответствует количеству открытых сессий. Оранжевый цвет пиктограммы и фона обозначают сессию локального администратора. Знак вопроса означает, что права пользователя не определены
	На компьютере (компьютерах) действует фильтр событий тревоги
	На компьютерах, подчиненных серверу безопасности, зафиксированы ошибки (красный цвет пиктограммы) или предупреждения (желтый цвет) при проверке лицензий на использование компонентов системы Secret Net Studio
	База данных сервера безопасности переполнена
	Учетная запись компьютера отключена

Пиктограммы приведены в порядке уменьшения приоритета отображения. В элементах диаграммы в первую очередь отображаются пиктограммы с более высоким приоритетом. Если в элементе не хватает отведенной зоны для вывода всех пиктограмм, исключаются наименее значимые.

Сведения в иерархическом списке объектов управления

В панели "Компьютеры" при отображении списка объектов управления сведения о состоянии объектов представлены в табличном виде. Включение табличного режима отображения осуществляется с помощью кнопки "Таблица" в верхней части панели "Компьютеры".

Пример списка объектов управления в табличном виде представлен на рисунке.



Сведения о компьютерах и серверах безопасности отображаются в колонках:

Пиктограмма включенного состояния
Содержит пиктограмму, если компьютер или сервер включен. Дополнительно имя включенного компьютера отображается полужирным шрифтом, а цвет его пиктограммы меняется на зеленый при отсутствии на компьютере тревог и запросов на утверждение аппаратной конфигурации
Высокий, Повышенный, Низкий
Содержит количество событий тревоги, произошедших на защищаемом компьютере и ожидающих квитирования (подтверждение приема) администратором безопасности. В колонке "Высокий" указано количество критических событий тревоги (с уровнем тревоги "высокий"). В остальных колонках — количество менее значимых событий тревоги (с уровнями тревоги "повышенный" и "низкий" соответственно). Дополнительно цвет пиктограммы компьютера в колонке "Имя" меняется на цвет тревоги наивысшего уровня, ожидающей квитирования
Пиктограмма блокировки
Содержит пиктограмму включенной блокировки, если компьютер заблокирован. Чтобы получить дополнительные сведения о причине блокировки, наведите указатель на ячейку — информация будет выведена во всплывающем сообщении рядом с курсором
ФК
Содержит пиктограмму, соответствующую результату проведения функционального контроля при запуске компьютера. Чтобы получить дополнительные сведения, наведите указатель на ячейку — информация появится во всплывающем сообщении рядом с ним
Сессии
Содержит краткие сведения об активных сессиях или имя пользователя, открывшего сессию. Чтобы получить дополнительные сведения, наведите указатель на ячейку — информация будет выведена во всплывающем сообщении рядом с курсором
Последнее подключение
Содержит время последнего подключения к серверу безопасности для выключенного компьютера
Лицензии
Содержит пиктограммы, если зафиксированы ошибки (красный цвет пиктограммы) или предупреждения (желтый цвет) при проверке лицензий на использование компонентов системы Secret Net Studio. Количество ошибок или предупреждений указывается рядом с пиктограммой
Домен безопасности
Содержит имя домена безопасности, к которому относится объект
Тип
Содержит пиктограмму операционной системы, установленной на компьютере
Версия
Содержит номер версии установленного программного обеспечения Secret Net Studio (ПО сервера безопасности или клиента)
Уровень важности
Содержит общий уровень важности компьютера
Полнодисковое шифрование
Содержит количество зашифрованных дисков и пиктограмму, показывающую, зашифрован ли системный диск

Управление отображением сведений в списке объектов управления

Сведения о состоянии объектов управления можно сортировать по содержимому колонок таблицы. Сортировка выполняется стандартными методами с помощью заголовков колонок.

При необходимости также можно изменять состав отображаемых колонок таблицы и порядок их следования. Чтобы настроить колонки, вызовите контекстное меню в строке заголовков, выберите команду "Настройка колонок" и в появившемся диалоге сформируйте список отображаемых колонок.

Печать и экспорт сведений о компьютерах

Программа позволяет отправлять на печать и/или сохранять (экспортировать) сведения о компьютерах, которые отображаются в списке объектов управления.

Экспорт сведений осуществляется в файлы форматов RTF и CSV. Для загрузки содержимого RTF- файлов и CSV- файлов необходимо использовать соответствующие приложения, поддерживающие возможность просмотра таких файлов. Например, редактор Microsoft Word и электронная таблица Microsoft Excel.

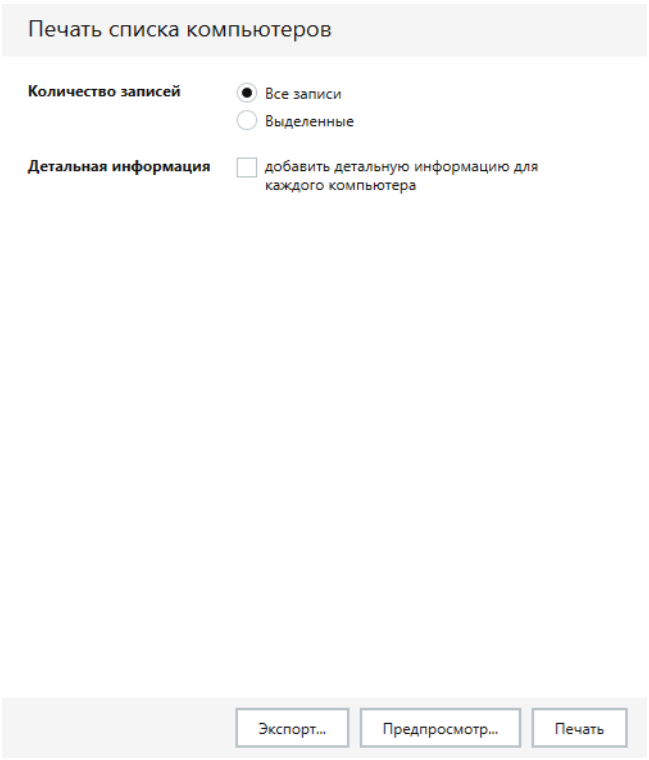
Внимание! Не рекомендуется загружать полученный файл во встроенный редактор ОС Windows WordPad, так как в этом редакторе возможны искажения оформления. При отсутствии редактора Microsoft Word для просмотра и печати RTF-файлов можно использовать средство просмотра Word Viewer. Данное приложение распространяется бесплатно и доступно для загрузки на веб-узле компании Microsoft.

Настройка параметров печати и экспорта осуществляется в специальной панели настройки.

Для печати или экспорта сведений:

1. Подготовьте таблицу со списком объектов управления для вывода данных: настройте отображение сведений (при необходимости) и не отключайте отображение серверов и компьютеров в таблице.
2. Если нужно распечатать или сохранить сведения по отдельным компьютерам из числа отображаемых, выделите нужные компьютеры в таблице.
3.  В верхней части панели "Компьютеры" нажмите кнопку "Печать".

   На экране появится панель настройки параметров.



4. Настройте параметры вывода сведений.

Группа полей "Количество записей"
Определяет, какие записи о компьютерах будут распечатаны или сохранены: • "Все записи" — операция выполняется для всех компьютеров списка; • "Выделенные" — операция выполняется только для тех компьютеров, которые выделены в таблице
Поле "Детальная информация"
Если установлена отметка, для компьютеров дополнительно будут приведены сведения, не указанные явно в таблице (например, причина блокировки)

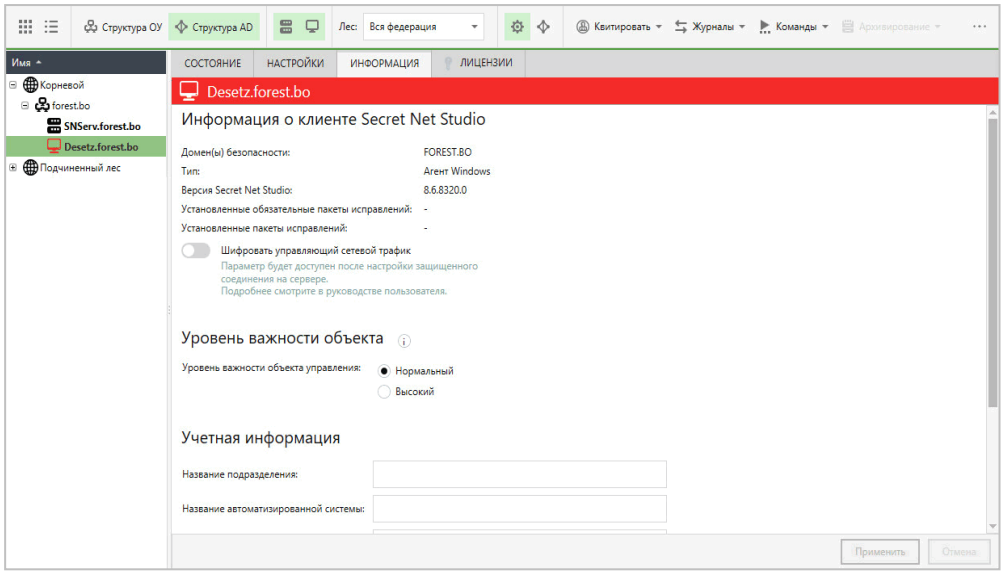
5. Чтобы открыть окно предварительного просмотра страниц, нажмите кнопку "Предпросмотр" в нижней части панели настройки параметров печати. После просмотра подготовленных сведений закройте окно.

Примечание. В окне предварительного просмотра можно отправить документ на печать с помощью стандартной кнопки на панели инструментов.

6. В нижней части панели настройки параметров нажмите нужную кнопку:
   - чтобы запустить процесс печати — нажмите кнопку "Печать" и укажите общие параметры печати (выбранный принтер, число копий и др.) в диалоге настройки ОС Windows;
   - чтобы сохранить сведения в файле — нажмите кнопку "Экспорт" и укажите имя и тип файла в диалоге сохранения файла ОС Windows.

Сведения о состоянии объектов

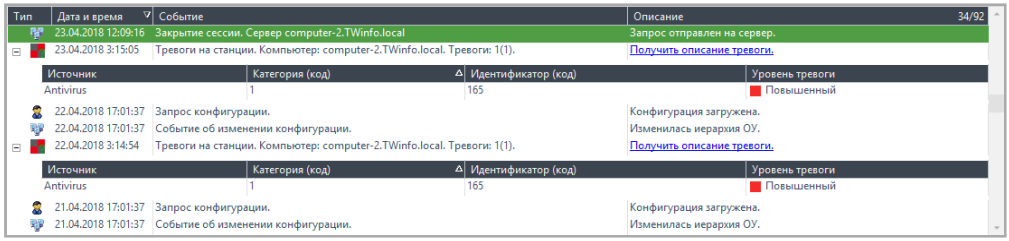
Вывод сведений о состоянии объектов осуществляется в панели "Компьютеры" на вкладке "Информация". При включении отображения сведений панель "Компьютеры" имеет вид, подобный представленному на рисунке.



На вкладке "Информация" представлены основные сведения об объекте и домене безопасности, к которому он относится. Средства для управления объектом доступны на вкладке "Состояние".

Сведения в панели событий системы

Панель событий системы может использоваться для получения сведений об изменении состояния защищаемых компьютеров. Пример содержимого панели представлен на следующем рисунке.



В панели событий системы могут выводиться сведения следующих типов:

- "События сети" — уведомления об изменении состояния контролируемых объектов, их конфигурации и о связи с сервером безопасности (например, "*<имя_компьютера>* заблокирован", "Потеряна связь с сервером..." и др.);
- "Действия пользователя" — уведомления, информирующие о действиях пользователей (например, "Команда "заблокировать" отправлена для агента (ов)...", "Квитирование тревог для агентов..." и др.);
- "Тревоги" — уведомления о фактах регистрации событий тревоги на защищаемых компьютерах (например, "Тревоги на станции").

Если не заданы особые цвета для уведомлений, сведения, полученные во время текущей сессии работы с программой, отображаются на белом фоне. Сведения других сессий — на сером фоне.

Параметры отображения данных в панели событий можно изменять (см. стр.**123**).

Просмотр расширенной информации о событиях

В панели событий системы может выводиться расширенная информация о событиях. Например, в уведомлениях о событиях изменения политики контроля устройств или о событиях тревоги. Расширенная информация выводится в виде табличного блока, для отображения которого используется кнопка раскрытия иерархии в левой части строки.

Табличный блок уведомления об изменении политики содержит список политик и их измененных значений. Для событий тревоги выводятся основные сведения, полученные в уведомлениях. Чтобы загрузить все сведения о событиях тревоги в блоке, выберите ссылку "Получить описание тревоги" — в блок будут загружены сведения в виде записей журнала с описанием событий. При просмотре записей могут использоваться те же функции настройки отображения, как и в основной таблице с записями журнала (сортировка, группировка, выбор колонок и др.).

Предусмотрена возможность отображения дополнительных данных о событии. Для этого вызовите контекстное меню записи о событии и выберите команду "Детально" — в правой части панели событий системы откроется панель детального описания. Если данные о событии содержат информацию о каком-либо устройстве, можно скопировать эту информацию в буфер обмена, чтобы потом добавить устройство с этими параметрами в групповую политику. Действие выполняется с помощью команды "Копировать устройство" в контекстном меню панели детального описания.

Автоматическое отображение последних сведений

Новые уведомления о событиях помещаются в конец списка. Для удобства просмотра актуальных сведений предусмотрен режим автоматического прокручивания списка к последнему добавленному элементу.

Для включения этого режима вызовите контекстное меню в любом месте панели событий системы и выберите команду "Автоматическая прокрутка".

Экспорт сведений

Программа позволяет сохранять (экспортировать) в файлы сведения, отображаемые в панели событий системы. Экспорт выполняется в файлы формата XML.

Экспорт осуществляется с помощью команд контекстного меню "Экспорт" и "Экспортировать все". Команда "Экспорт" применяется, чтобы экспортировать отдельные выбранные строки таблицы сведений. Если требуется экспортировать всю таблицу, вызовите контекстное меню в любом месте панели событий системы и выберите команду "Экспортировать все".

Отслеживание событий тревоги

Центр управления информирует о событиях, на которые необходимо обратить внимание администратора безопасности (события тревоги). Такие события регистрируются на защищаемых компьютерах в журнале Secret Net Studio или штатном журнале безопасности ОС и имеют тип "Аудит отказов" или "Ошибки".

События тревоги различаются по степени значимости самих событий и уровню важности объекта, на котором они произошли. Критические события могут иметь уровень тревоги "высокий" для объектов с высоким уровнем важности или "повышенный" — для объектов с нормальным уровнем важности. Менее значимые события имеют уровень тревоги "повышенный" или "низкий" соответственно уровню важности объектов.

Сервер безопасности накапливает сведения о событиях тревоги в отдельном журнале. Журнал событий тревоги формируется из уведомлений, направляемых серверу от защищаемых компьютеров.

Оповещение о событиях тревоги

При получении уведомлений о произошедших событиях тревоги Центр управления незамедлительно оповещает пользователя об этом. Оповещение происходит путем подачи различных визуальных сигналов. Например, соответствующие элементы диаграммы управления выделяются красным цветом. Также для оповещения могут использоваться и звуковые сигналы.

Отключение оповещения и возвращение обычного вида объектов происходит после квитирования событий тревоги.

Статистические сведения о неквитированных событиях тревоги выводятся на панели "Статистика" в виде списков, показателей и графиков распределения событий.

Квитирование событий тревоги

Внимание! Квитирование событий тревоги необходимо выполнять до архивирования журнала событий тревоги. Если в архив были помещены записи, не прошедшие процедуру квитирования, значение счетчика событий тревоги уменьшается, и администратор безопасности может пропустить информацию о несанкционированном доступе. В этом случае для квитирования событий следует восстановить журнал событий тревоги из архива в базу данных сервера безопасности, после чего появится возможность обработать информацию в обычном порядке.

Под квитированием событий тревоги понимается подтверждение о получении информации администратором безопасности с описанием принятых мер. Как правило, каждое событие тревоги требует выяснения причин его возникновения и выполнения экстренных действий для обеспечения безопасности информационной системы. После того как администратор безопасности принял к сведению и проанализировал обстоятельства возникновения события тревоги, необходимо подтвердить прием информации, выполнив процедуру квитирования.

При квитировании администратор вводит текстовый комментарий с описанием причин и принятых мер, и этот комментарий сохраняется в системе вместе с признаком квитирования события. Информация о самом событии тревоги не удаляется из журнала. В дальнейшем по журналу событий тревоги можно определить, кто, когда и как отреагировал на произошедшие события. После квитирования всех событий, полученных от компьютера, этому объекту возвращается нормальный вид отображения.

Примечание. Помимо квитирования событий тревоги с обязательным вводом комментария администратором безопасности, в Центре управления предусмотрена возможность сброса счетчиков событий (см. ниже). Процедура сброса счетчиков предназначена только для случаев, связанных с настройкой системы защиты, и не должна применяться в штатном режиме функционирования.

Квитирование событий тревоги выполняется при работе с журналом событий тревоги в панели "Журналы тревог" (см. стр.**206**).

Сброс счетчиков событий тревоги

При получении уведомлений о зарегистрированных событиях тревоги счетчики событий и измененные пиктограммы объектов отображаются до тех пор, пока не будут обнулены значения счетчиков для этих объектов.

Уменьшение значений счетчиков происходит при квитировании событий тревоги (см. выше). В штатном режиме функционирования системы защиты обнуление счетчиков необходимо выполнять только посредством квитирования событий, так как процедура квитирования предусматривает просмотр информации о событиях и добавление уточняющих комментариев администратора безопасности.

Во время настройки параметров системы защиты на этапе пробной эксплуатации допускается сбрасывать значения счетчиков событий тревоги для оперативного возврата к нормальному виду отображения объектов. При сбросе счетчиков система воспринимает в качестве принятых к сведению все события тревоги, произошедшие на защищаемом компьютере (компьютерах) на момент поступления команды. Однако в отличие от процедуры квитирования при сбросе счетчиков не запрашивается уточняющий комментарий администратора безопасности. При этом в системе сохраняются сведения о том, кто и когда выполнил обнуление значений, вместе с информацией о событиях тревоги.

Для сброса счетчиков событий тревоги:

1. В диаграмме управления или в списке объектов выберите нужные объекты.

2. Вызовите контекстное меню одного из выбранных объектов, раскройте подменю "Квитировать" и выберите нужную команду:
   - "Все тревоги" — для квитирования всех событий независимо от уровней тревоги;
   - "Тревоги высокого уровня" — для квитирования только событий с уровнем тревоги "высокий";
   - "Тревоги повышенного уровня" — для квитирования только событий с уровнем тревоги "повышенный";
   - "Тревоги низкого уровня" — для квитирования только событий с уровнем тревоги "низкий".
3. При появлении диалога запроса на продолжение действия подтвердите выполнение операции.

   Для объектов будет возвращен нормальный вид отображения. О результатах выполнения действия выводится уведомление в панели событий системы.

Создание правил фильтрации на основе уведомлений о событиях тревоги

Для выборочного отслеживания событий можно настроить фильтр, который будет определять, какие уведомления о событиях тревоги должны поступать на сервер безопасности. Фильтр тревог действует независимо от политики регистрации событий в локальных журналах, что дает возможность контроля важных изменений в системе без уменьшения объема сохраняемой информации в локальных журналах. Фильтр может применяться при передаче уведомлений от защищаемых компьютеров на сервер безопасности (настраивается в группе "Оповещения о тревогах" раздела "Политики" панели свойств объектов), а также при передаче уведомлений, полученных подчиненными серверами безопасности (настраивается в разделе "Параметры").

В создаваемых правилах автоматически добавляются условия фильтрации на основе выбранных сведений. Создание правил в панели событий предусмотрено для уведомлений о событиях тревоги, полученных во время текущей сессии работы с программой.

Для добавления правила в панели событий системы:

1. В панели событий системы перейдите к уведомлению о событиях тревоги и раскройте блок с расширенной информацией о событиях. Для этого наведите указатель на строку уведомления и дважды нажмите левую кнопку мыши или нажмите кнопку раскрытия иерархии в левой части строки.

   Примечание. Описание панели событий системы и возможностей для управления отображением сведений см. на стр. 175.
2. В блоке с расширенной информацией вызовите контекстное меню события и раскройте подменю "Добавить правило для фильтрации тревоги".
3. Выберите команду добавления правила в нужный фильтр. Фильтр событий тревоги может быть задан в групповых политиках (при наличии возможности изменения политик) или в параметрах сервера безопасности.

   После выбора команды в панели "Компьютеры" будет открыта соответствующая группа параметров, и в списке правил фильтра появится новое правило. Если добавляемое правило может повлиять на применение ранее заданных параметров, перед добавлением на экране появится запрос на выполнение дальнейших действий. В этом случае перед продолжением операции рекомендуется проверить заданные параметры.

Оперативное управление

Оперативное управление защищаемыми компьютерами осуществляется с помощью команд. Команды оперативного управления могут применяться к компьютерам как самого сервера подключения (сервер безопасности, с которым установлено соединение Центра управления), так и подчиненных серверов. При этом выбранный для управления компьютер должен быть включен.

Примечание. Если в данный момент исполнение какой-либо оперативной команды невозможно, эта команда или отсутствует в меню, или неактивна.

Управление пользовательскими сессиями

Для включенных компьютеров можно просматривать информацию о текущих пользовательских сессиях, а также завершать выбранные сессии.

Для завершения пользовательских сессий:

1. В диаграмме управления или в списке объектов выберите нужный компьютер.
2. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Состояние" и нажмите плитку "Вход в систему".

   Справа отобразится блок с информацией о механизме и списком пользовательских сессий на компьютере.
3. Выберите пользовательские сессии, которые требуется завершить. Для выбора нескольких сессий используйте вместе с мышью клавиши "Shift" и "Ctrl". Нажмите кнопку "Завершить сессию", которая расположена над списком сессий.

Блокировка и разблокирование компьютеров

Включенные компьютеры можно удаленно заблокировать или снять блокировку (разблокировать). Команды для выполнения действий могут применяться к компьютерам или серверам безопасности. Если команда применяется для сервера безопасности, соответствующее действие будет выполнено для всех компьютеров, подчиненных данному серверу.

При поступлении команды блокировки на экране компьютера появляется сообщение об этом и прерывается сеанс работы текущего пользователя. Одновременно в журнале Secret Net Studio регистрируется событие "Компьютер заблокирован системой защиты", которое является событием тревоги. Локально разблокировать компьютер может только пользователь, входящий в локальную группу администраторов.

Если компьютер заблокирован системой защиты, соответствующие объекты в Центре управления отображаются с измененными пиктограммами (см. стр.**170**). Для такого компьютера может применяться команда разблокирования. После получения команды на разблокирование на экране компьютера появляется сообщение об этом и пользователь может продолжить работу.

Для блокировки компьютеров:

1. В диаграмме управления или в списке объектов выберите нужный объект (компьютер, группа, сервер безопасности) или выделите несколько нужных объектов.
2. Вызовите контекстное меню выбранного объекта (одного из выделенных объектов), раскройте подменю "Команды" и выберите команду "Заблокировать". При появлении диалога запроса на продолжение действия подтвердите выполнение операции.

Для разблокирования компьютеров:

1. В диаграмме управления или в списке объектов выберите нужный объект

(компьютер, группа, сервер безопасности) или выделите несколько нужных объектов.

2. Вызовите контекстное меню выбранного объекта (одного из выделенных объектов), раскройте подменю "Команды" и выберите команду "Разблокировать". При появлении диалога запроса на продолжение действия подтвердите выполнение операции.

Примечание. Заблокировать или разблокировать компьютер можно также на вкладке "Состояние" данного компьютера. Выберите элемент "Блокировка" и нажмите кнопку "Заблокировать" или "Разблокировать" соответственно.

Перезагрузка и выключение компьютеров

Для включенных компьютеров можно удаленно инициировать перезагрузку или выключение. Команды для выполнения действий могут применяться к компьютерам или серверам безопасности. Если команда применяется для сервера безопасности, соответствующее действие (перезагрузка или выключение) будет выполнено для всех компьютеров, подчиненных данному серверу.

Перезагрузка или выключение компьютера выполняется независимо от количества открытых приложений и наличия несохраненных документов. При поступлении команды на экране компьютера появляется сообщение об этом, и в течение 15 секунд с момента появления сообщения пользователь компьютера может сохранить открытые документы.

Для перезагрузки или выключения компьютеров:

1. В диаграмме управления или в списке объектов выберите нужный объект (компьютер, группа, сервер безопасности) или выделите несколько нужных объектов.
2. Вызовите контекстное меню выбранного объекта (одного из выделенных объектов), раскройте подменю "Команды" и выберите команду "Перезагрузить" или "Выключить" для перезагрузки или выключения компьютера соответственно. При появлении диалога запроса на продолжение действия подтвердите выполнение операции.

Обновление групповых политик на компьютерах

Для включенных компьютеров можно удаленно инициировать запуск обновления групповых политик. Команда применяется к отдельным компьютерам, серверам безопасности и группам компьютеров. Если выбран сервер безопасности или группа, обновление групповых политик выполняется на всех компьютерах под управлением ОС Windows, подчиненных серверу безопасности или включенных в группу.

Принудительное обновление ускоряет процесс применения централизованно заданных групповых политик на компьютерах.

Для обновления групповых политик на компьютерах:

1. В диаграмме управления или в списке объектов выберите нужный объект (компьютер, группа, сервер безопасности) или выделите несколько нужных объектов.
2. Вызовите контекстное меню выбранного объекта (одного из выделенных объектов), раскройте подменю "Команды" и выберите команду "Применить групповые политики".

Утверждение изменений аппаратной конфигурации

Для включенных компьютеров можно удаленно утвердить изменения аппаратной конфигурации. Команда утверждения конфигурации применяется только к компьютерам под управлением ОС Windows.

Компьютер, на котором зафиксировано изменение аппаратной конфигурации, обозначается в диаграмме управления специальной пиктограммой (см. стр.170).

Для утверждения аппаратной конфигурации на компьютере:

1. Вызовите контекстное меню компьютера с измененной аппаратной конфигурацией и выберите команду "Утвердить аппаратную конфигурацию".

   На экране появится диалог со списком устройств, не совпадающих с эталонной аппаратной конфигурацией компьютера.

2. Для учета изменений в составе эталонной аппаратной конфигурации компьютера нажмите кнопку "Утвердить".

Примечание. Утвердить аппаратную конфигурацию можно также следующими способами:

- на вкладке "Состояние" выбранного компьютера выберите элемент "Контроль устройств" и нажмите кнопку "Утвердить аппаратную конфигурацию";
- в панели событий системы вызовите контекстное меню уведомления "На агенте <*имя_компьютера*> изменилась аппаратная конфигурация" и выберите команду "Утвердить аппаратную конфигурацию".

Сбор локальных журналов по команде администратора

Передача локальных журналов защищаемых компьютеров в БД сервера безопасности выполняется регулярно в соответствии с заданными параметрами (см. стр.**148**).

Для включенных компьютеров можно выполнить запуск процесса внеочередной передачи локальных журналов. Команды применяются к отдельным компьютерам, серверам безопасности и группам компьютеров. Если выбран сервер безопасности или группа, сбор локальных журналов выполняется со всех компьютеров, подчиненных серверу безопасности или включенных в группу.

Для запуска процесса передачи локальных журналов:

1. В диаграмме управления или в списке объектов выберите нужные объекты.
2. Вызовите контекстное меню одного из выбранных объектов, раскройте подменю "Журналы / Собрать журналы с компьютера".
3. Выберите команду с названием нужного журнала или команду "Все", если требуется передать в БД сервера безопасности все локальные журналы.

   В панели событий системы появится уведомление о запуске процесса сбора локальных журналов. Статус выполнения процесса отображается в колонке "Описание".

Управление функционированием механизмов защиты на компьютерах

Для включенных компьютеров можно использовать средства оперативной настройки функционирования механизмов защиты.

Для настройки функционирования механизмов защиты на компьютере:

1. В диаграмме управления или в списке объектов выберите нужный объект.
2. Включите отображение параметров объекта (с помощью команды "Свойства" в контекстном меню) и перейдите на вкладку "Состояние" (см. стр.**174**).

   Примечание. При выборе нескольких объектов вкладка "Состояние" недоступна.

3. Нажмите кнопку нужного механизма (например, "Затирание данных").

   Справа от кнопки появится блок, содержащий сведения о механизме.

4. Чтобы включить или отключить механизм защиты, переведите в нужное положение переключатель, расположенный слева в заголовке блока. При появлении диалога запроса на продолжение действия подтвердите выполнение операции.

Примечание. Включение механизма защиты возможно при наличии действующей лицензии для данного механизма. Выключатель присутствует в заголовке блока, если лицензия на данный механизм включена. Управление списком лицензий осуществляется на вкладке "Лицензии".

5. Если для механизма предусмотрены дополнительные возможности настройки, выполните нужные действия с помощью средств управления, представленных в блоке.

Запуск программы удаленного управления компьютером

Центр управления предоставляет возможность запуска программы PuTTY, используемой для подключения к компьютерам под управлением ОС Linux с установленным ПО Secret Net LSP и отправки команд управления по протоколу Secure Shell (SSH). Ввод команд управления осуществляется в режиме командной строки в отдельном окне программы PuTTY.

Для использования программы на компьютерах должны быть установлены соответствующие части программного обеспечения:

- на рабочем месте администратора — программа PuTTY (SSH-клиент). Если файл putty.exe находится не в каталоге установки Центра управления, необходимо задать путь к файлу в параметрах работы Центра управления (см. стр.**123**);
- на защищаемом компьютере — сервер для входящих SSH-подключений. На компьютере под управлением ОС Linux с установленным ПО Secret Net LSP компоненты SSH-сервера функционируют по умолчанию и дополнительная установка не требуется. На компьютере под управлением ОС Windows SSH-сервер по умолчанию не установлен. Для подключения необходимо установить ПО сервера (например, Bitvise SSH Server).

Для запуска программы удаленного управления:

1. Вызовите контекстное меню компьютера под управлением ОС Linux с установленным ПО Secret Net LSP и выберите команду "Запустить удаленное управление через PuTTY".

   На экране появится диалог для ввода имени и пароля пользователя с правами на удаленное управление.
2. Введите имя и пароль пользователя (например, локального администратора компьютера, к которому выполняется подключение) и нажмите кнопку "Запустить".

   На экране появится окно программы PuTTY. После установления соединения с компьютером в окне появится приглашение на ввод команды.
3. Введите нужную команду (команды). Действия в окне программы PuTTY выполняются так же, как и в локальной консоли командной строки.

Формирование отчетов

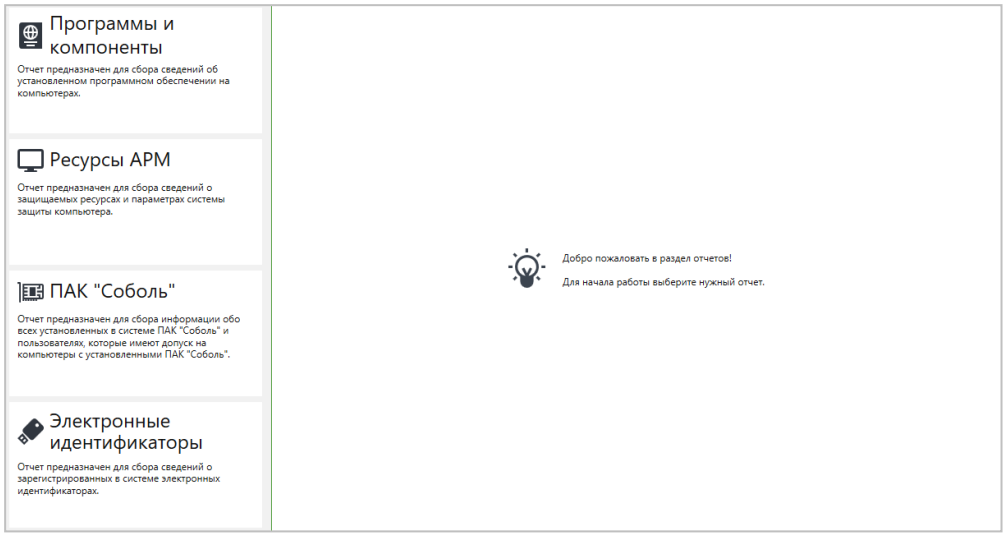
В Центре управления можно формировать следующие отчеты:

Название	Описание
Программы и компоненты	Содержит учетную информацию компьютеров и перечень установленного на них программного обеспечения
Ресурсы АРМ	Содержит учетную информацию компьютеров и подробные сведения о параметрах установленной на них системы защиты
Допуск пользователей в ПАК "Соболь"	Содержит сведения об установленных ПАК "Соболь" и список пользователей, имеющих допуск к компьютерам с ПАК "Соболь"
Электронные идентификаторы	Содержит сведения об электронных идентификаторах, зарегистрированных в Secret Net Studio

Примечание. В Локальном центре управления можно сформировать только отчеты "Программы и компоненты" и "Ресурсы АРМ".

Создание запросов для формирования отчетов выполняется в панели "Отчеты", для перехода к которой нажмите кнопку "Отчеты" на панели навигации (слева в основном окне). Отчеты формируются только для компьютеров под управлением ОС Windows.

В режиме ожидания запроса панель имеет следующий вид.



Для отчетов могут быть заданы общие параметры оформления: название и логотип организации, а также параметры нумерации страниц.

Отчеты сохраняются в файлы формата RTF. Для загрузки содержимого RTF-файлов необходимо использовать соответствующие приложения, поддерживающие возможность просмотра таких файлов. Например, редактор Microsoft Word или средство просмотра Word Viewer. Вместе с отчетом доступно сохранение данных в файле формата XML.

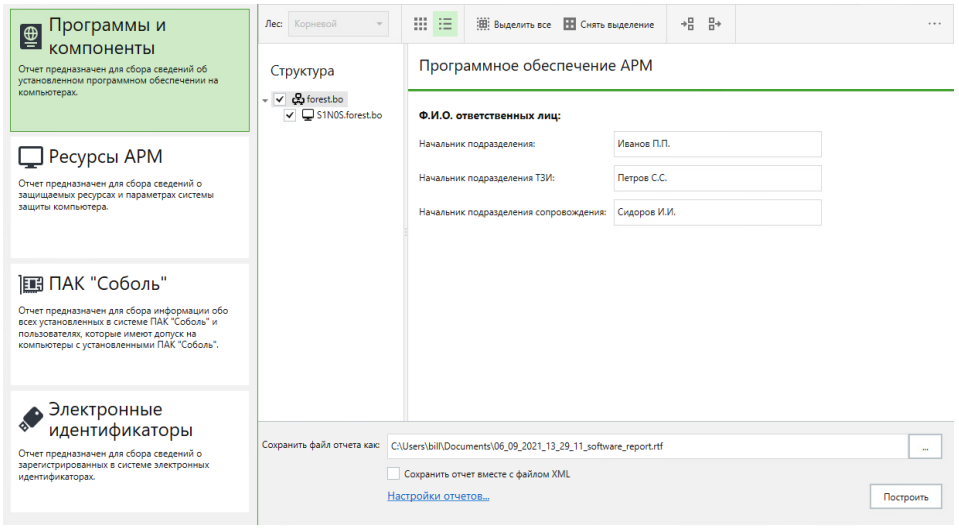
Отчет "Программы и компоненты"

Отчет со сведениями о программном обеспечении, установленном на компьютерах, формируется только для включенных компьютеров.

Для формирования отчета:

1. В левой части панели "Отчеты" выберите раздел "Программы и компоненты".

   Панель примет вид, подобный представленному на следующем рисунке.



В списке "Структура" представлены защищаемые компьютеры, сведения о которых можно добавить в отчет. Список содержит только включенные в данный момент компьютеры.

Совет.

- Список может содержать простой перечень компьютеров или иерархию объектов в структуре Active Directory. Переключение режима отображения списка осуществляется с помощью соответствующих кнопок, расположенных над списком.
- Также список можно отфильтровать по именам объектов. Чтобы отобразить в списке нужные компьютеры, в строке поиска введите строку символов, которая должна присутствовать в именах компьютеров или других объектов.

2. Отметьте компьютеры, сведения о которых требуется получить в отчете.

Совет.

- Чтобы установить или удалить отметки одновременно для всех компьютеров, используйте соответствующие кнопки в верхней части панели.
- Предварительный выбор компьютеров для формирования отчета можно выполнить в диаграмме управления или в списке объектов панели "Компьютеры". Действия выполняются аналогично командам оперативного управления. Чтобы перейти к формированию запроса на построение отчета для нужных компьютеров, используйте команду "Отчеты | Программы и компоненты" в контекстном меню объектов.

3. В правой части панели "Отчеты" введите в соответствующих полях ФИО сотрудников, ответственных за эксплуатацию выбранных компьютеров.
4. В поле "Сохранить файл отчета как" введите полное имя файла отчета или нажмите кнопку в правой части поля, чтобы указать файл в диалоге сохранения файла ОС Windows.
5. При необходимости поставьте отметку в поле "Сохранить отчет вместе с файлом XML" и настройте общие параметры оформления отчета: название и логотип организации, а также параметры нумерации страниц. Чтобы изменить общие параметры, выберите ссылку "Настройки отчетов", укажите нужные значения в появившемся диалоге и нажмите кнопку "ОК".
6. Нажмите кнопку "Построить".

   Начнется процесс получения и обработки данных. По завершении подготовки отчета на экране появится соответствующее сообщение. Чтобы загрузить полученный файл отчета, нажмите кнопку "Просмотр".

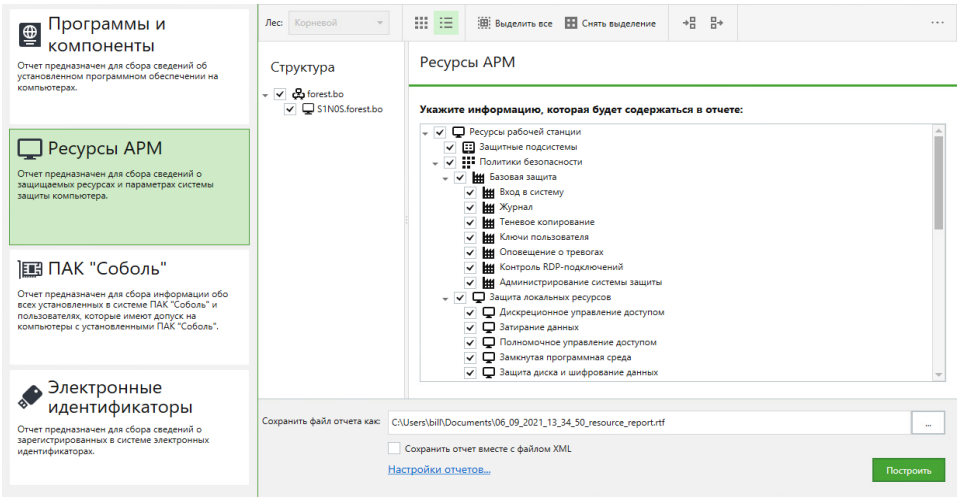
Отчет "Ресурсы АРМ"

Отчет со сведениями о параметрах системы защиты формируется только для включенных компьютеров.

Для формирования отчета:

1. В левой части панели "Отчеты" выберите раздел "Ресурсы АРМ".

   Панель примет вид, подобный представленному на следующем рисунке.



В списке "Структура" представлены защищаемые компьютеры, сведения о которых можно добавить в отчет. Список содержит только включенные в данный момент компьютеры.

Совет.

- Список может содержать простой перечень компьютеров или иерархию объектов в структуре Active Directory. Переключение режима отображения списка осуществляется с помощью соответствующих кнопок, расположенных над списком.
- Также список можно отфильтровать по именам объектов. Чтобы отобразить в списке нужные компьютеры, в строке поиска введите строку символов, которая должна присутствовать в именах компьютеров или других объектов.

2. Отметьте компьютеры, сведения о которых требуется получить в отчете.

Совет.

- Чтобы установить или удалить отметки одновременно для всех компьютеров, используйте соответствующие кнопки в верхней части панели.
- Предварительный выбор компьютеров для формирования отчета можно выполнить в диаграмме управления или в списке объектов панели "Компьютеры". Действия выполняются аналогично командам оперативного управления. Чтобы перейти к формированию запроса на построение отчета для нужных компьютеров, используйте команду "Отчеты | Ресурсы АРМ" в контекстном меню объектов.

3. В правой части панели "Отчеты" отметьте разделы сведений, которые необходимо включить в отчет.

Название	Описание
Защитные подсистемы	Раздел в отчете содержит перечень защитных подсистем Secret Net Studio – C. Для каждой подсистемы указывается информация о лицензии и текущем состоянии подсистемы
Политики безопасности	Раздел в отчете содержит параметры указанных политик безопасности. Для получения отдельных сведений отметьте подчиненные элементы с названиями нужных групп параметров
Регистрация событий	Раздел в отчете содержит перечень событий и параметры их регистрации
Параметры	Раздел в отчете содержит параметры сетевых настроек и параметры сбора журналов
Локальные пользователи	Раздел в отчете содержит информацию о локальных пользователях компьютера
Локальные группы пользователей	Раздел в отчете содержит информацию о локальных группах пользователей

Название	Описание
Доменные пользователи, заходившие на компьютер	Раздел в отчете содержит информацию о доменных пользователях, выполнивших вход на компьютер
Задания контроля целостности	Раздел в отчете содержит информацию об имеющихся на компьютере заданиях контроля целостности и списках ресурсов этих заданий
Задания Замкнутой программной среды	Раздел в отчете содержит информацию об имеющихся на компьютере заданиях замкнутой программной среды и списках ресурсов этих заданий
Дискреционное управление доступом	Раздел в отчете содержит информацию о контролируемых этим механизмом ресурсах и установленных для них параметрах безопасности
Ресурсы полномочного управления доступом	Раздел в отчете содержит список конфиденциальных ресурсов и сведения об установленных для них параметрах безопасности
Ресурсы зашифрованных данных	Раздел в отчете содержит список имеющихся криптоконтейнеров с указанием их параметров

4. В поле "Сохранить файл отчета как" введите полное имя файла отчета или нажмите кнопку в правой части поля, чтобы указать файл в диалоге сохранения файла ОС Windows.
5. При необходимости поставьте отметку в поле "Сохранить отчет вместе с файлом XML" и настройте общие параметры оформления отчета: название и логотип организации, а также параметры нумерации страниц. Чтобы изменить общие параметры, выберите ссылку "Настройки отчетов", укажите нужные значения в появившемся диалоге и нажмите кнопку "ОК".
6. Нажмите кнопку "Построить".

   Начнется процесс получения и обработки данных. По завершении подготовки отчета на экране появится соответствующее сообщение. Чтобы загрузить полученный файл отчета, нажмите кнопку "Просмотр".

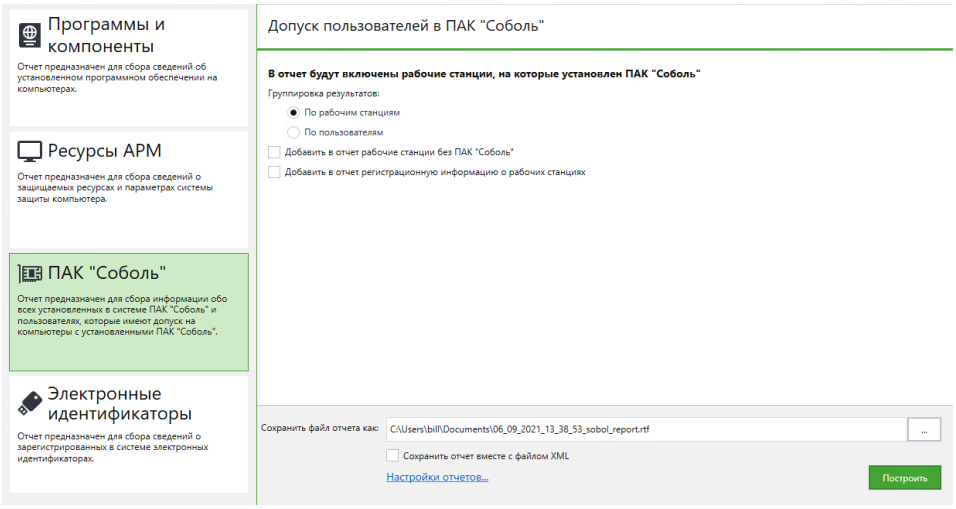
Отчет "Допуск пользователей в ПАК "Соболь"

Отчет со сведениями об установленных ПАК "Соболь" и списком пользователей, имеющих допуск к компьютерам с ПАК "Соболь", формируется по информации, которая хранится на сервере безопасности.

Для формирования отчета:

1. В левой части панели "Отчеты" выберите раздел "ПАК "Соболь".

   Панель примет вид, подобный представленному на следующем рисунке.



Совет. При работе с объектами в диаграмме управления или в списке объектов панели "Компьютеры" можно перейти к формированию отчета "Допуск пользователей в ПАК "Соболь" с помощью команды контекстного меню "Отчеты | ПАК "Соболь".

2. Выберите нужный вариант группировки сведений в отчете. Сведения могут быть представлены по компьютерам или по пользователям. Для выбора варианта группировки установите отметку в соответствующем поле.
3. Если требуется, чтобы в отчете дополнительно были представлены сведения о компьютерах, на которых не установлен ПАК "Соболь", установите отметку в поле "Добавить в отчет рабочие станции без ПАК "Соболь".
4. Если требуется добавить в отчет учетную информацию для каждого компьютера (сведения о рабочем месте, номер системного блока и др.), установите отметку в поле "Добавить в отчет регистрационную информацию о рабочих станциях".
5. В поле "Сохранить файл отчета как" введите полное имя файла отчета или нажмите кнопку в правой части поля, чтобы указать файл в диалоге сохранения файла ОС Windows.
6. При необходимости поставьте отметку в поле "Сохранить отчет вместе с файлом XML" и настройте общие параметры оформления отчета: название и логотип организации, а также параметры нумерации страниц. Чтобы изменить общие параметры, выберите ссылку "Настройки отчетов", укажите нужные значения в появившемся диалоге и нажмите кнопку "ОК".
7. Нажмите кнопку "Построить".

   Начнется процесс получения и обработки данных. По завершении подготовки отчета на экране появится соответствующее сообщение. Чтобы загрузить полученный файл отчета, нажмите кнопку "Просмотр".

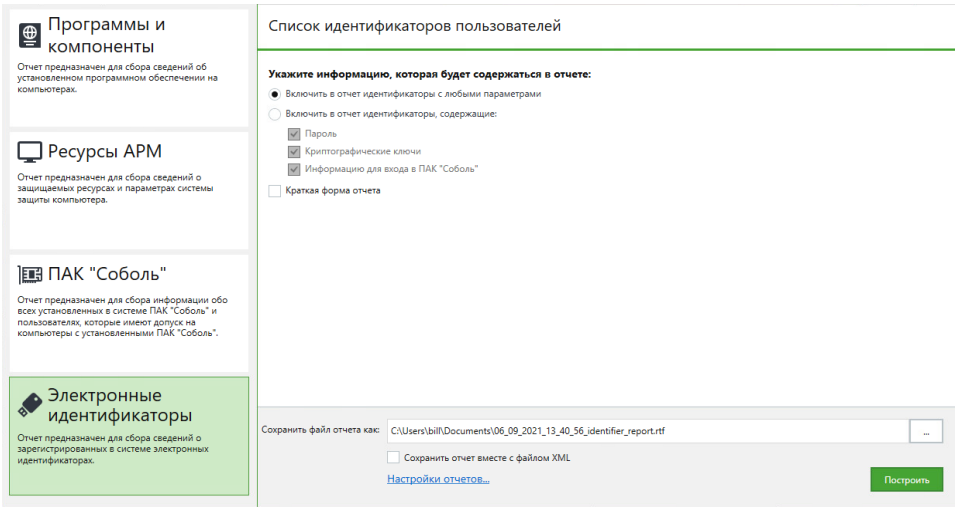
Отчет "Электронные идентификаторы"

Отчет со сведениями об электронных идентификаторах, зарегистрированных в Secret Net Studio, формируется по информации, которая хранится на сервере безопасности.

Для формирования отчета:

1. В левой части панели "Отчеты" выберите раздел "Электронные идентификаторы".

   Панель примет вид, подобный представленному на следующем рисунке.



Совет. При работе с объектами в диаграмме управления или в списке объектов панели "Компьютеры" можно перейти к формированию отчета "Электронные идентификаторы" с помощью одноименной команды в подменю "Отчеты" контекстного меню.

2. Если требуется, чтобы в отчете были представлены идентификаторы, содержащие любые параметры, установите отметку в поле "Включить в отчет идентификаторы с любыми параметрами".
3. Если требуется отфильтровать идентификаторы в зависимости от содержащихся в них данных (паролей пользователей, криптографических ключей или данных для работы с ПАК "Соболь"), установите отметку в поле "Включить в отчет идентификаторы, содержащие" и отметьте нужные типы данных. В отчете будут представлены те идентификаторы, которые содержат данные любого типа из числа отмеченных.
4. По умолчанию для каждого идентификатора в отчете представлен перечень всех типов данных, которые могут быть записаны. При необходимости сохранить в отчете только сведения об имеющихся данных установите отметку в поле "Краткая форма отчета".
5. В поле "Сохранить файл отчета как" введите полное имя файла отчета или нажмите кнопку в правой части поля, чтобы указать файл в диалоге сохранения файла ОС Windows.
6. При необходимости поставьте отметку в поле "Сохранить отчет вместе с файлом XML" и настройте общие параметры оформления отчета: название и логотип организации, а также параметры нумерации страниц. Чтобы изменить общие параметры, выберите ссылку "Настройки отчетов", укажите нужные значения в появившемся диалоге и нажмите кнопку "ОК".
7. Нажмите кнопку "Построить".

   Начнется процесс получения и обработки данных. По завершении подготовки отчета на экране появится соответствующее сообщение. Чтобы загрузить полученный файл отчета, нажмите кнопку "Просмотр".

Глава 16
Работа с централизованными журналами

Возможность загрузки централизованных журналов из базы данных сервера безопасности доступна при подключении программы к серверу. Загрузку записей из файлов можно выполнять при работе программы как с подключением к серверу безопасности, так и в автономном режиме.

Имеется возможность по мере сбора журналов Secret Net Studio с рабочих станций оперативно предоставлять полную информацию из этих журналов SIEM-системам (см. стр.**294**).

Централизованные журналы

В базе данных сервера безопасности накапливаются следующие журналы:

- журнал событий тревоги, объединяющий все записи о событиях тревоги со всех управляемых компьютеров;
- журнал событий, объединяющий журнал Secret Net Studio и штатные журналы ОС Windows со всех управляемых компьютеров;
- журнал сервера безопасности.

Информацию из этих журналов можно загружать частично или полностью в Центр управления.

Журнал событий тревоги

Журнал событий тревоги предназначен для централизованного хранения информации о событиях тревоги, произошедших на защищаемых компьютерах. Событиями тревоги считаются события, которые регистрируются локально в журнале Secret Net Studio или штатном журнале безопасности ОС и имеют тип "Аудит отказов" или "Ошибки". Журнал событий тревоги формируется из уведомлений о событиях тревоги, направляемых серверу безопасности.

Сведения, содержащиеся в журнале событий тревоги, позволяют администратору безопасности оперативно получать наиболее важную информацию о попытках несанкционированного доступа в системе. При возникновении события тревоги сведения о нем регистрируются в соответствующем локальном журнале и одновременно отправляются серверу безопасности, который сохраняет их в журнале событий тревоги. Таким образом, в системе дублируются сведения о таком событии, что уменьшает риск потери информации.

Для компьютеров может действовать фильтр событий тревоги, который определяет критерии выборочного отслеживания событий. Если правила фильтрации не заданы, в журнал событий тревоги поступает информация о каждом событии тревоги на компьютере.

Сведения о событиях сохраняются в журнале в виде записей. Каждая запись включает в себя набор полей с данными из локального журнала, а также поля с дополнительными данными (тип локального журнала, сведения об агенте, уровень угрозы, квитирование и другие параметры).

Объединенный журнал компьютеров

Объединенный журнал компьютеров (называемый также журнал станций) предназначен для централизованного хранения содержимого локальных журналов, поступивших с защищаемых компьютеров. К локальным журналам относятся журнал Secret Net Studio и штатные журналы ОС Windows (журнал приложений, системный журнал и журнал безопасности). Описание назначения локальных журналов см. в документе [**2**], глава "Локальный аудит".

Передача локальных журналов для централизованного хранения в базу данных сервера безопасности осуществляется в соответствии с заданными параметрами (см. стр.148).

Сведения, полученные из локальных журналов, сохраняются в полном объеме в объединенном журнале. Вместе с этими сведениями в каждой записи о событии фиксируются дополнительные данные (тип локального журнала, сведения об агенте, уровень угрозы и другие параметры).

Журнал сервера безопасности

В журнале сервера безопасности протоколируются сессии доступа к серверу, открываемые компонентами и программами Secret Net Studio, включая внутренние сессии самого сервера безопасности.

Сведения о сессиях сохраняются в журнале в виде записей. Каждая запись включает в себя набор полей, в которых представлены следующие данные:

- общие данные о сессии: имя компьютера, инициаторы открытия (компонент и пользователь), время открытия и закрытия сессии;
- основные данные о выполнявшихся действиях в сессии: время выполнения каждого действия, результат, описание самого действия;
- дополнительные данные с детальными описаниями событий (системные идентификаторы объектов, кодовые обозначения результатов и другие параметры).

Хранение журналов

Журналы с записями о событиях могут храниться в следующих хранилищах:

- локальные хранилища на компьютерах, где были зарегистрированы события (локальные журналы);
- централизованное хранилище в БД сервера безопасности;
- файлы архивов, созданных сервером безопасности.

В Центре управления осуществляется просмотр журналов, хранящихся в централизованном хранилище или в файлах архивов. Для просмотра текущего содержимого локальных журналов требуется предварительная передача журналов на хранение в БД сервера безопасности.

Локальные хранилища журналов

При регистрации событий записи о них помещаются в соответствующие локальные журналы и хранятся на защищаемом компьютере. Пока записи хранятся в локальном хранилище, их можно загрузить локально на компьютере.

Локальные журналы хранятся до тех пор, пока они не будут переданы в централизованное хранилище на сервере безопасности. После передачи записей происходит очистка содержимого локальных журналов.

Внимание! При работе с локальными журналами пользователь, наделенный соответствующими полномочиями, может выполнять очистку журналов до их передачи на сервер безопасности. Чтобы исключить возможность несанкционированного удаления информации, необходимо предоставлять полномочия управления локальными журналами только доверенным пользователям.

Централизованное хранилище

Централизованное хранилище журналов размещается в БД сервера безопасности. Сведения о событиях, регистрируемых в журнале событий тревоги или в журнале сервера безопасности, поступают непосредственно в централизованное хранилище без промежуточного размещения в других хранилищах. В объединенном журнале компьютеров размещается содержимое локальных журналов при их передаче из локальных хранилищ в БД сервера безопасности. Запуск процесса передачи локальных журналов с защищаемых компьютеров осуществляется в следующих случаях:

- в моменты времени, заданные параметрами автоматической передачи журналов (см. стр.**148**);
- по команде пользователя Центра управления (см. стр.**181**).

Примечание. Для штатных журналов ОС Windows можно отключить передачу записей в централизованное хранилище. Если для журнала отключена функция централизованного сбора, этот журнал игнорируется при запросе локальных журналов и содержимое этого журнала остается в локальном хранилище.

Удаление записей журналов из централизованного хранилища происходит при архивировании журналов.

Просмотр и управление записями журналов, хранящихся в БД сервера безопасности, осуществляется только в Центре управления.

Архивы журналов, созданные сервером безопасности

Для уменьшения объема базы данных сервера безопасности предусмотрена возможность архивирования содержимого централизованных журналов. Архивируются все записи журналов, имеющиеся в БД сервера безопасности на момент начала процесса архивирования (для журнала сервера безопасности — архивируются сведения о завершенных сессиях). Записи, помещенные в архив, удаляются из централизованного хранилища.

Запуск процесса архивирования осуществляется в следующих случаях:

- в моменты времени, заданные параметрами автоматического архивирования журналов (см. стр.**150**);
- по команде пользователя Центра управления (см. стр.**209**).

Архивированные записи журналов хранятся в файлах. Для каждого архива создается отдельный файл. По умолчанию для размещения архивов используется подкаталог \Archive, расположенный в каталоге установки сервера безопасности.

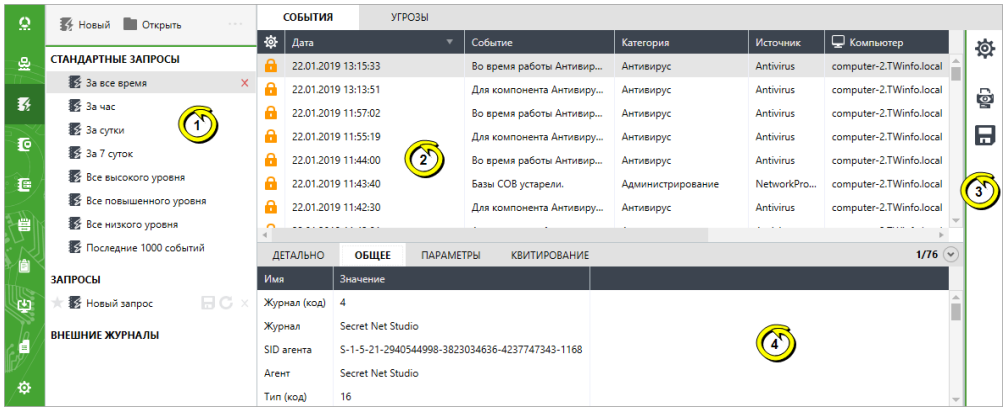
Панели для работы с записями журналов

Вывод записей централизованных журналов осуществляется в следующих панелях:

- панель журнала событий тревоги. Во время работы с программой переход к панели журнала осуществляется с помощью ярлыка "Журналы тревог" в панели навигации или по ссылке "Журнал получен" в уведомлении о запросе журнала в панели событий системы;
- панель журнала станций. Во время работы с программой переход к панели журналов осуществляется с помощью ярлыка "Журналы станций" в панели навигации или по ссылке "Журнал получен" в уведомлении о запросе журнала событий в панели событий системы;
- панель журнала сервера безопасности. Во время работы с программой переход к панели журналов осуществляется с помощью ярлыка "Журналы сервера" в панели навигации или по ссылке "Журнал получен" в уведомлении о запросе журнала сервера в панели событий системы;
- панель архивов журналов — открывается по умолчанию, если при запуске Центра управления в диалоге выбора режима работы выбрана команда запуска в автономном режиме "Архив журналов" и указан файл архива для загрузки. Во время работы с программой переход к панели архивов осуществляется с помощью ярлыка "Архивы" в панели навигации.

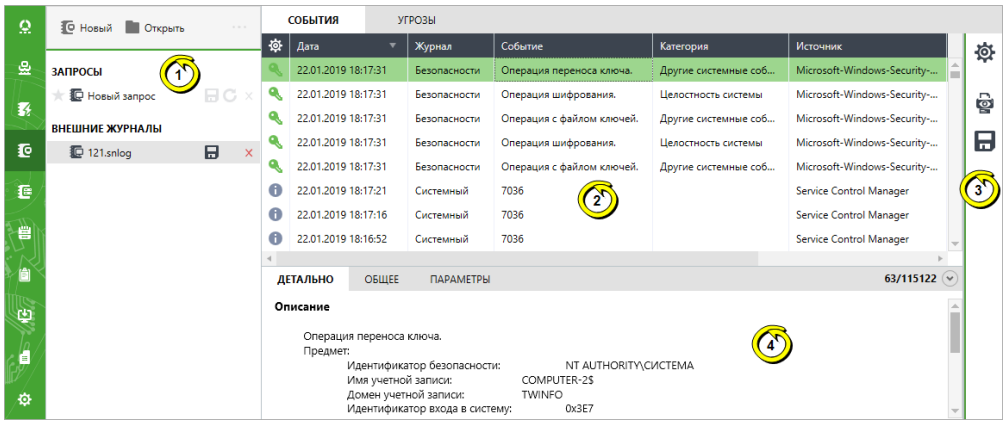
Для загрузки записей в панели создается вкладка, называемая запросом. В панели можно работать с несколькими запросами. Переходы между ними осуществляются посредством выбора нужного запроса в панели управления запросами.

Панель журнала событий тревоги имеет вид, подобный представленному на следующем рисунке.



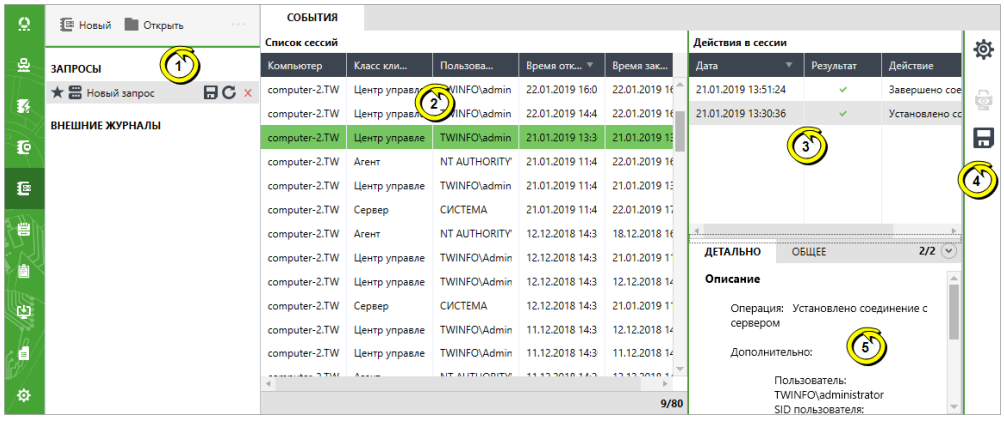
Пояснение. На рисунке обозначены: 1 — панель управления запросами; 2 — область отображения сведений; 3 — панель настройки вывода сведений; 4 — область описания событий.

Панель журнала станций имеет вид, подобный представленному на следующем рисунке.



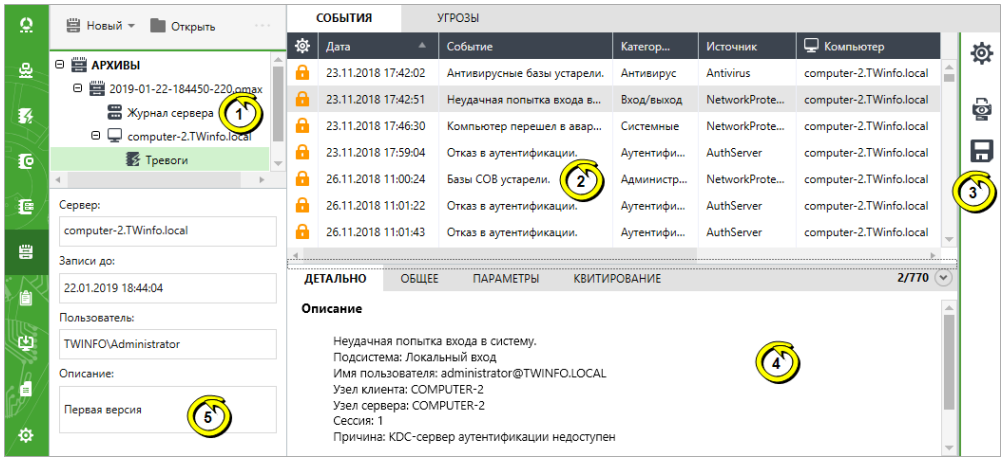
Пояснение. На рисунке обозначены: 1 — панель управления запросами; 2 — область отображения сведений; 3 — панель управления записями; 4 — область описания событий.

Панель журнала сервера безопасности имеет вид, подобный представленному на следующем рисунке.



Пояснение. На рисунке обозначены: 1 — панель управления запросами; 2 — область отображения списка сессий; 3 — область отображения сведений о выбранной сессии; 4 — панель настройки вывода сведений; 5 — область описания событий.

Пример панели архивов журналов представлен на следующем рисунке.



Пояснение. На рисунке обозначены: 1 — панель управления запросами; 2 — область отображения сведений; 3 — панель настройки вывода сведений; 4 — область описания событий; 5 — область основных сведений об архиве.

Основные элементы интерфейса:

Панель управления запросами

Содержит списки запросов для загрузки записей. Запросы группируются в следующих разделах:

- "Стандартные запросы" — запросы с предопределенными критериями отбора записей, загружаемых из журнала (только для журнала событий тревоги);
- "Запросы" — запросы, созданные пользователем для загрузки записей из журнала;
- "Внешние журналы" — запросы, созданные при загрузке записей из файлов;
- "Архивы" — запросы, полученные по результатам анализа содержимого загруженных архивов

Область отображения сведений

Содержит сведения о событиях в журнале в виде таблицы со списком записей. В таблице можно изменять состав отображаемых колонок и порядок их следования. Чтобы настроить колонки, вызовите контекстное меню в строке заголовков, выберите команду "Настройка колонок" и в появившемся диалоге сформируйте список отображаемых кнопок

Панель настройки вывода сведений

Содержит кнопки вызова средств конфигурирования запроса, печати и экспорта записей

Область описания событий

Содержит подробную информацию о выбранном событии. Информация о событиях группируется в следующих вкладках:

- "Детально" — содержит детальное описание и полученные данные. Если данные о событии содержат информацию о каком-либо устройстве, можно скопировать эту информацию в буфер обмена, чтобы потом добавить устройство с этими параметрами в групповую политику;
- "Общее" — содержит полный список полей и их значений в записи о зарегистрированном событии. Список представлен в табличной форме;
- "Параметры" — содержит список параметров системы Secret Net Studio, полученных из детального описания события. Список представлен в табличной форме;
- "Квитирование" — содержит сведения о том, кто и когда выполнил процедуру квитирования (подтверждение приема) для выбранной записи, и текстовый комментарий с описанием действий. Вкладка отображается только для журнала событий тревоги при выборе записи с признаком квитирования.

Включение и отключение области описания событий осуществляется при выборе команды "Детально" в контекстном меню записи о событии или с помощью кнопки, расположенной справа в нижней строке области отображения сведений

Область основных сведений об архиве

Используется только в панели архивов журналов. Содержит основные сведения о выбранном архиве, сохраненные при его создании: имя сервера безопасности, граница интервала времени для записей, имя создавшего архив пользователя, описание архива

Загрузка записей журналов

Запросы для журнала событий тревоги

В Центре управления предусмотрены следующие способы создания запросов на загрузку записей журнала событий тревоги:

- создание запросов по статистическим данным;
- контекстное создание запросов для объектов;
- создание запросов с предопределенными критериями отбора;
- создание запросов с произвольными критериями отбора;
- создание запросов на загрузку записей журнала из файлов.

Создание запросов по статистическим данным

Статистические данные о событиях тревоги представлены в панели "Статистика". Также в правом верхнем углу основного окна Центра управления отображается индикатор состояния системы, который содержит общее количество событий тревоги (при наличии неквитированных событий).

Счетчики количества событий тревоги в панели "Статистика" и в индикаторе состояния системы могут использоваться для создания запросов на загрузку записей журнала событий тревоги. Чтобы создать новый запрос, выберите значение нужного счетчика. В панели журнала событий тревоги появится новый запрос, в котором автоматически будет выполнена загрузка записей.

Контекстное создание запросов для объектов

Запросы на загрузку записей журнала событий тревоги можно создавать применительно к объектам, выбранным в панели диаграммы управления или в списке объектов. Для таких запросов автоматически создаются правила отбора и фильтрации по контексту выбранных объектов и команд.

Для контекстного создания запроса:

1. В диаграмме управления или в списке объектов выберите нужные объекты.

   Примечание. О наличии зарегистрированных событий тревоги, ожидающих квитирования (подтверждения приема) администратором безопасности, оповещают счетчики событий, которые отображаются рядом с объектами (см. стр.170 и стр.171).

2. Вызовите контекстное меню одного из выбранных объектов, раскройте подменю "Журналы / Журнал тревог" и выберите нужную команду:
   - "Все тревоги" — для получения сведений о событиях всех уровней тревоги;
   - "Тревоги высокого уровня", "Тревоги повышенного уровня", "Тревоги низкого уровня" — для получения сведений только о событиях с соответствующим уровнем тревоги.

   По окончании загрузки записей в панели событий системы появится уведомление о получении журнала. Для перехода к записям журнала выберите в уведомлении ссылку "Журнал получен".

Создание запросов с предопределенными критериями отбора

Запросы с предопределенными критериями отбора позволяют оперативно загрузить в Центр управления неквитированные записи о событиях тревоги, которые были зарегистрированы в течение заданного периода времени или имеют определенный уровень тревоги.

Создание запросов с предопределенными критериями отбора выполняется в панели журнала. Такие запросы целесообразно создавать при наличии в системе неквитированных записей о событиях тревоги.

Для создания запроса с предопределенными критериями отбора:

- В разделе "Стандартные запросы" панели управления запросами наведите указатель на элемент списка, соответствующий нужному периоду времени или уровню важности событий, и дважды нажмите левую кнопку мыши.

  В панели журнала будет создан новый запрос с соответствующими параметрами, после чего автоматически инициируется процесс получения записей из журнала. По окончании загрузки записей в панели событий системы появится уведомление о получении журнала со ссылкой для перехода к новому запросу.

Создание запросов с произвольными критериями отбора

Запросы с произвольными критериями отбора записей создаются для последующей настройки параметров и запуска процесса получения записей вручную.

Создание запросов выполняется в панели журнала событий тревоги.

Для создания запроса:

1. В панели управления запросами нажмите кнопку "Новый".

   В панели журнала будет создан новый запрос, и справа появится панель для настройки его параметров.

2. Настройте параметры нового запроса (см. стр.**199**) и нажмите кнопку "Выполнить запрос к БД" в нижней части панели настройки параметров.

   Будет инициирован процесс получения записей из журнала. По окончании загрузки записей в панели событий системы появится уведомление о получении журнала со ссылкой для перехода к новому запросу.

Создание запросов на загрузку записей журнала событий тревоги из файлов

Записи журнала событий тревоги могут храниться в файлах формата *.snua. Загрузка записей из таких файлов в панель журнала событий тревоги осуществляется путем создания отдельных запросов для каждого файла.

Файл для загрузки можно указать при запуске Центра управления в автономном режиме (см. стр.**121**) или во время работы с Центром управления в панели журнала событий тревоги.

Для создания запроса на загрузку записей из файла в панели журнала событий тревоги:

1. В панели управления запросами нажмите кнопку "Открыть".

   На экране появится диалог открытия файла ОС Windows.

2. Выберите нужный файл.

   В панели журнала будет создан новый запрос, в который будут загружены записи из файла.

Запросы для журнала станций

В Центре управления предусмотрены следующие способы создания запросов на загрузку записей журнала станций:

- контекстное создание запросов для объектов;
- создание запросов с произвольными критериями отбора;
- создание запросов на загрузку записей журнала станций или локальных журналов из файлов.

Контекстное создание запросов для объектов

Запросы на загрузку записей журнала станций можно создавать применительно к объектам, выбранным в панели диаграммы управления или в списке объектов. Для таких запросов автоматически создаются правила отбора и фильтрации по контексту выбранных объектов и команд.

Для контекстного создания запроса:

1. В диаграмме управления или в списке объектов выберите нужные объекты.
2. Вызовите контекстное меню одного из выбранных объектов, раскройте подменю "Журналы / Журналы компьютеров из БД" и выберите команду, соответствующую нужным критериям отбора записей. Можно загрузить записи о событиях, поступившие из определенных локальных журналов по отдельности или журнала Secret Net Studio совместно с журналом безопасности. По команде "Создать запрос" выполняется создание запроса с переходом в панель "Журналы станций" для настройки параметров запроса (см. стр.**199**).

   После выбора команды на загрузку записей о событиях, поступивших из определенных локальных журналов, автоматически инициируется процесс получения записей из журнала станций. По окончании загрузки записей в панели событий системы появится уведомление о получении журнала. Для перехода к записям журнала выберите в уведомлении ссылку "Журнал получен".

Создание запросов с произвольными критериями отбора

Запросы с произвольными критериями отбора записей создаются для последующей настройки параметров и запуска процесса получения записей вручную.

Создание запросов для загрузки записей журнала станций выполняется в панели "Журналы станций".

Для создания запроса:

1. В панели управления запросами нажмите кнопку "Новый".

   В панели "Журналы станций" будет создан новый запрос, и справа появится панель для настройки его параметров.
2. Настройте параметры нового запроса (см. стр.**199**) и нажмите кнопку "Выполнить запрос к БД" в нижней части панели настройки параметров запроса.

   Будет инициирован процесс получения записей из журнала. По окончании загрузки записей в панели событий системы появится уведомление о получении журнала со ссылкой для перехода к новому запросу.

Создание запросов на загрузку записей журнала станций или локальных журналов из файлов

Записи журнала станций могут храниться в файлах специального формата *.snlog. Загрузка записей из таких файлов в панель "Журналы станций" осуществляется путем создания отдельных запросов для каждого файла.

Кроме того, отдельные запросы, аналогичные запросам на загрузку журнала станций, можно создавать для файлов стандартного формата журнала событий ОС Windows *.evt*.

Файл для загрузки можно указать при запуске Центра управления в автономном режиме (см. стр.**121**) или во время работы в панели "Журналы станций".

Для создания запроса на загрузку записей из файла в панели "Журналы станций":

1. В панели управления запросами нажмите кнопку "Открыть".

   На экране появится диалог открытия файла ОС Windows.
2. Выберите нужный файл.

В панели "Журналы станций" будет создан новый запрос, в который будут загружены записи из файла.

Запросы для журнала сервера безопасности

В Центре управления предусмотрены следующие способы создания запросов на загрузку записей журнала сервера безопасности:

- контекстное создание запросов;
- создание запросов с произвольными критериями отбора;
- создание запросов на загрузку записей журнала сервера безопасности из файлов.

Контекстное создание запросов

Запросы на загрузку записей журнала сервера безопасности можно создавать при работе в панели диаграммы управления или в списке объектов. Для таких запросов автоматически могут создаваться правила отбора и фильтрации по контексту выбранных команд.

Для контекстного создания запроса:

1. В диаграмме управления или в списке объектов вызовите контекстное меню сервера безопасности, журнал которого требуется загрузить. В контекстном меню раскройте подменю "Журналы / Журналы сервера".
2. Выберите команду, соответствующую нужным критериям отбора записей. Можно загрузить записи о событиях, зарегистрированных в течение последнего часа, последних суток, или все записи. По команде "Создать запрос" выполняется создание запроса с переходом в панель "Журналы сервера" для настройки параметров запроса (см. стр.**199**).

   После выбора команды на загрузку записей о событиях, зарегистрированных в течение последнего часа, последних суток, или всех записей автоматически инициируется процесс получения записей из журнала сервера безопасности. По окончании загрузки записей в панели событий системы появится уведомление о получении журнала. Для перехода к записям журнала выберите в уведомлении ссылку "Журнал получен".

Создание запросов с произвольными критериями отбора

Запросы с произвольными критериями отбора записей создаются для последующей настройки параметров и запуска процесса получения записей вручную.

Создание запросов для загрузки записей журнала сервера безопасности выполняется в панели "Журналы сервера".

Для создания общего запроса:

1. В панели управления запросами нажмите кнопку "Новый".

   В панели "Журналы сервера" будет создан новый запрос, и справа появится панель для настройки его параметров.
2. Настройте параметры нового запроса (см. стр.**199**) и нажмите кнопку "Выполнить запрос к БД" в нижней части панели настройки параметров запроса.

   Будет инициирован процесс получения записей из журнала. По окончании загрузки записей в панели событий системы появится уведомление о получении журнала со ссылкой для перехода к новому запросу.

Создание запросов на загрузку записей журнала сервера безопасности из файлов

Записи журнала сервера безопасности могут храниться в файлах специального формата *.snsrv. Загрузка записей из таких файлов в панель "Журналы сервера" осуществляется путем создания отдельных запросов для каждого файла.

Файл для загрузки можно указать при запуске программы в автономном режиме (см. стр.**121**) или во время работы с программой в панели "Журналы сервера".

Для создания запроса на загрузку записей из файла в панели "Журнал сервера":

1. В панели управления запросами нажмите кнопку "Открыть".

   На экране появится диалог открытия файла ОС Windows.

2. Выберите нужный файл.

   В панели "Журналы сервера" будет создан новый запрос, в который будут загружены записи из файла.

Запросы для архивов журналов

Для просмотра записей журналов, помещенных в архивы, необходимо загрузить файлы нужных архивов в Центр управления.

Внимание! Для загрузки архивов требуется достаточное свободное пространство на диске, который используется для временных файлов (разархивирование осуществляется в папке временных файлов пользователя). Чтобы загружать архивы размером до 80–100 МБ, необходимо около 4 ГБ свободного пространства. Для работы с архивами размером 200–300 МБ требуется не менее 10 ГБ.

После загрузки архивов создаются запросы для отбора нужных записей. Создание запросов выполняется в панели "Архивы". В Центре управления предусмотрены следующие способы создания запросов:

- создание запроса для отбора записей отдельного журнала в загруженном архиве;
- создание запросов для отбора записей журнала событий тревоги или журнала станций в загруженных архивах.

Загрузка файлов архивов

Сервер безопасности создает архивы журналов в файлах специального формата *.omax.

Файлы архивов для загрузки можно указать при запуске Центра управления в автономном режиме (см. стр.121) или во время работы в панели "Архивы".

Примечание. В Центре управления поддерживается загрузка файлов архивов, созданных сервером безопасности СЗИ Secret Net версии 7.0 и выше.

Для загрузки файлов архивов в панели "Архивы":

1. В панели управления запросами нажмите кнопку "Открыть".

   На экране появится диалог открытия файла ОС Windows.

2. Выберите нужные файлы.

   В панели "Архивы" будут созданы новые подразделы, количество и названия которых соответствуют выбранным файлам архивов. Подразделы содержат иерархические списки компьютеров и журналов, записи которых получены из архивов. Основные сведения о загруженных архивах отображаются в области сведений, которая расположена под панелью управления запросами.

Создание запроса для отбора записей отдельного журнала в загруженном архиве

В загруженном архиве можно создавать запросы для отбора записей отдельных журналов, представленных в иерархическом списке архива. Такие запросы относятся только к выбранному журналу соответствующего компьютера и не допускают загрузку других записей, хранящихся в архиве.

Для создания запроса для отбора записей отдельного журнала:

1. В разделе "Архивы" панели управления запросами раскройте список подраздела с названием нужного архива.
2. Наведите указатель на строку журнала и дважды нажмите левую кнопку мыши.

В панели "Архивы" будет создан новый запрос, в котором отобразятся сведения из выбранного журнала.

Создание запроса для отбора записей журнала событий тревоги или журнала станций в загруженных архивах

Среди загруженных архивов можно сделать выборку из всех записей журналов событий тревоги или журналов станций, хранящихся в архивах. Запрос для отбора записей этих журналов позволяет получить записи, поступившие с различных компьютеров, и может применяться к нескольким выбранным архивам.

Для создания запроса для отбора записей журнала событий тревоги или журнала станций:

1. В панели управления запросами нажмите кнопку "Новый" и в появившемся меню выберите нужный тип запроса:
   - "Найти в журналах тревог" — создает запрос для выборки записей из журналов событий тревоги;
   - "Найти в журналах станций" — создает запрос для выборки записей из журналов станций.

   В панели "Архивы" будет создан новый запрос, и справа появится панель для настройки его параметров.
2. Настройте параметры нового запроса (см. стр.199) и нажмите кнопку "Найти в архивах" в нижней части панели настройки параметров запроса.

   Будет инициирован процесс получения записей из выбранных архивов.

Настройка параметров запроса

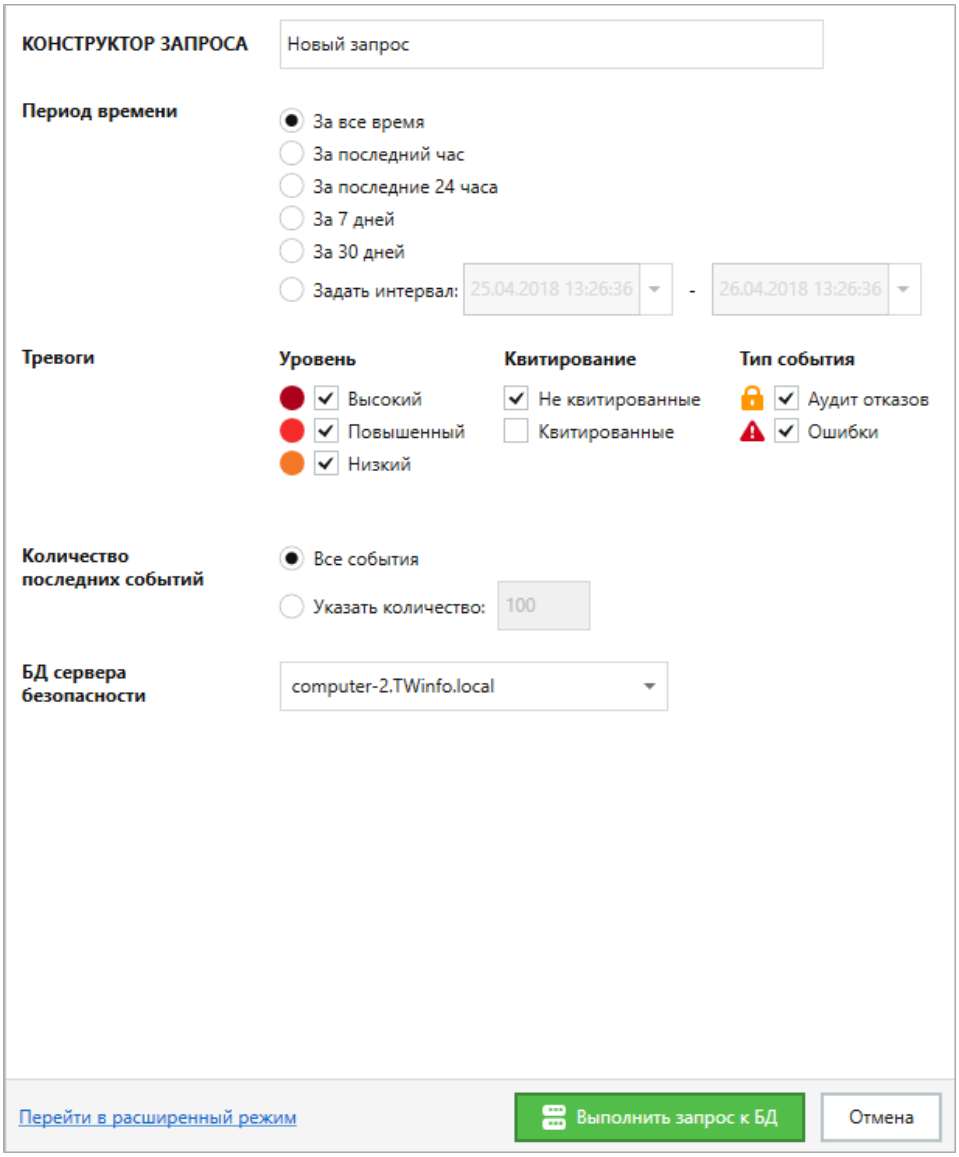
Для получения нужных сведений в запросе записей журнала можно изменять параметры загрузки и фильтрации записей. Настройка параметров осуществляется в специальной панели настройки.

Для настройки параметров запроса записей:

1. Включите отображение панели настройки параметров запроса. Чтобы включить или отключить отображение панели, используйте кнопку "Запрос" в панели настройки вывода сведений (справа от области отображения сведений).

   Примечание. Панель настройки параметров запроса отображается по умолчанию для созданного запроса с произвольными критериями отбора.

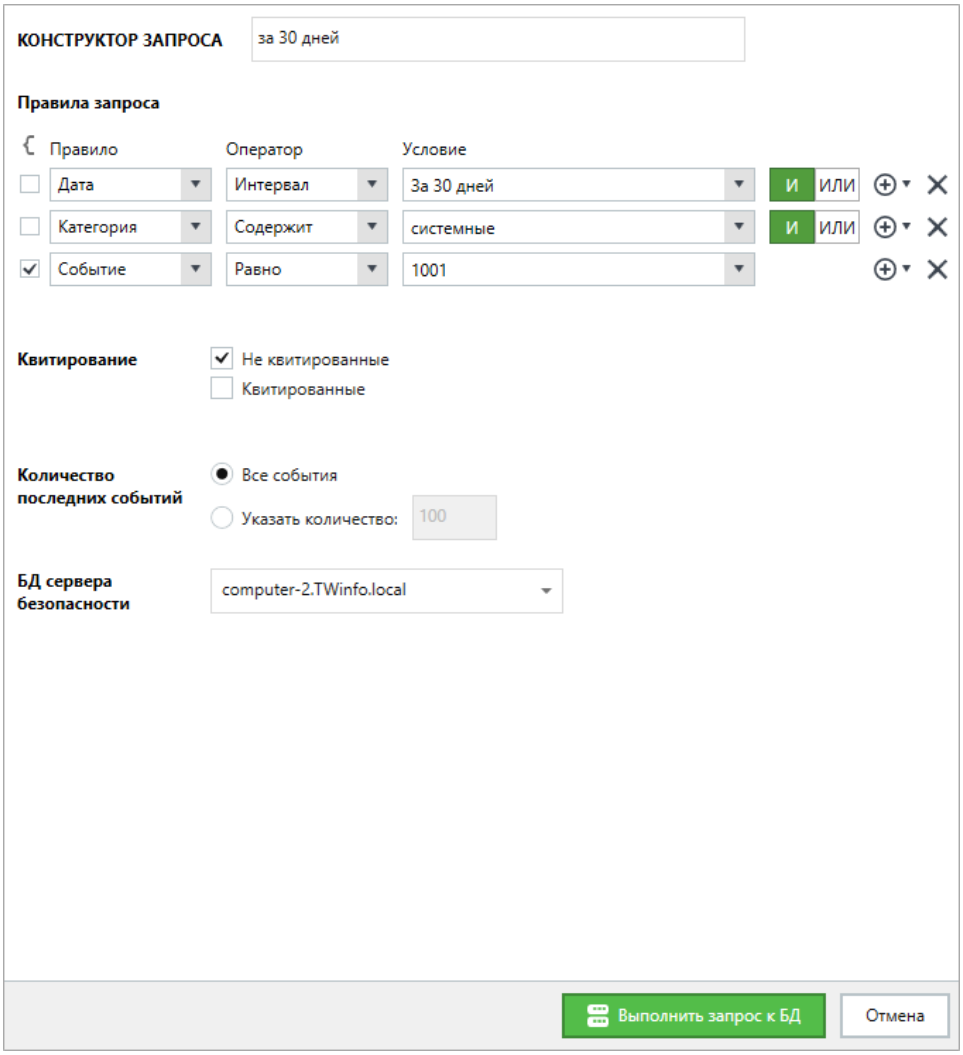
   Пример содержимого панели для журнала событий тревоги представлен на следующем рисунке.



2. Введите имя запроса и настройте параметры отбора записей в соответствующих полях. Состав настраиваемых параметров зависит от источника сведений, типов журналов и текущего режима панели настройки.

Для созданного запроса с произвольными критериями отбора по умолчанию панель представлена в упрощенном режиме, который позволяет указать основные параметры отбора записей (см. рисунок выше). При необходимости детализировать параметры включите расширенный режим настройки с помощью ссылки "Перейти в расширенный режим" в нижней части панели.

Пример содержимого панели в расширенном режиме настройки представлен на рисунке ниже.



3. Для применения заданных параметров используйте соответствующую кнопку в нижней части панели настройки:
   - Чтобы сделать новую выборку записей журнала из базы данных сервера безопасности, нажмите кнопку "Выполнить запрос к БД".
   - Чтобы выйти из настройки параметров запроса, нажмите кнопку "Отмена".

Управление запросами

В панелях "Журналы тревог", "Журналы станций" и "Журналы сервера" предусмотрены следующие возможности управления запросами (кроме запросов с предопределенными критериями отбора и запросов на загрузку из файлов):

- включение и отключение режима автоматической загрузки запроса;
- сохранение параметров запроса в файле;
- загрузка параметров запроса из файла;
- повторная загрузка записей из БД сервера безопасности.

Операции по управлению запросами выполняются с помощью кнопок в панели управления запросами. Средства управления перечислены в следующей таблице:

Кнопка	Описание
★	Включает и отключает режим автоматической загрузки запроса в следующих сеансах работы с программой. При включенном режиме кнопка выделена цветом

Кнопка	Описание
	Сохраняет выбранный запрос в файле. Сохранение осуществляется в файл формата *.snreq
	Запускает процесс новой загрузки записей в соответствии с текущими параметрами запроса
Открыть	Вызывает диалог открытия файла для загрузки запроса. Чтобы загрузить ранее сохраненный запрос, укажите тип файла "Запрос (*.snreq)". После загрузки запрос добавляется в раздел "Запросы" соответствующей панели журналов (в панель того журнала, для которого был создан запрос)

Для закрытия запроса используйте кнопку "Закрыть" справа от его названия.

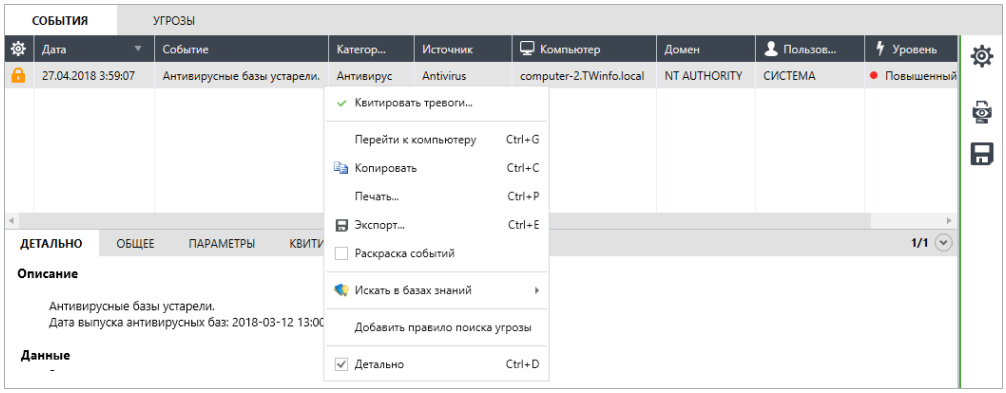
Возможности при просмотре записей

Режимы отображения сведений о событиях

Загруженная информация о событиях выводится в области отображения сведений соответствующей панели (см. стр. 191). Для анализа содержимого журналов предусмотрены различные режимы отображения сведений (кроме журнала сервера безопасности). Помимо вывода информации в виде обычного списка записей Центр управления предоставляет возможность просмотра сведений в виде списков событий угроз.

Режим "События"

В режиме "События" выводится список загруженных записей журналов в табличной форме. Это основной и наиболее функциональный режим для просмотра и управления записями. Пример содержимого окна с таблицей записей представлен на рисунке ниже.

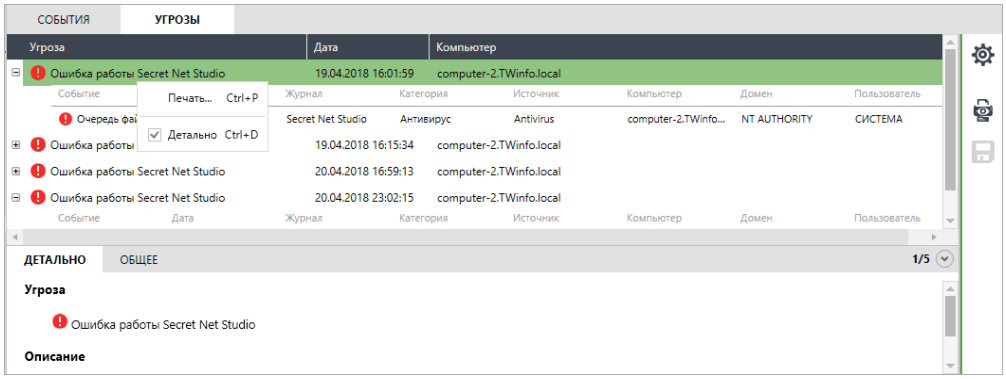


С помощью контекстного меню записей выполняются необходимые действия: копирование, печать, сохранение и др.

В правой части строки под таблицей содержится счетчик записей: <номер выбранной записи>/<количество выбранных записей>/<общее количество загруженных записей>.

Режим "Угрозы"

В режиме "Угрозы" выводится список событий угроз, полученных в результате анализа загруженных записей. События угроз представляют собой сжатые или разъясняющие сведения о зарегистрированных событиях (например, событие угрозы с признаками подбора пароля). Режим предназначен для представления администратору или аудитору наиболее важной для них информации из журналов. Пример содержимого окна с полученным списком представлен на рисунке ниже.



Информация выводится в табличной форме с возможностью раскрытия списков зарегистрированных событий, относящихся к событиям угроз. При просмотре табличных блоков с записями журналов могут использоваться те же функции настройки отображения, как и в основной таблице с записями журнала.

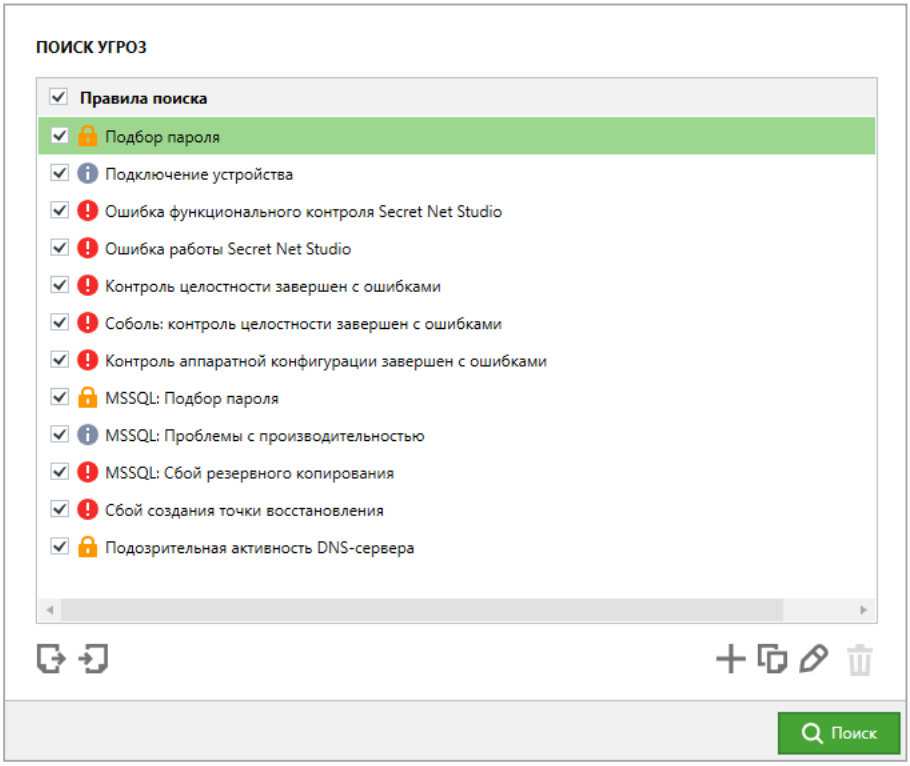
С помощью команд контекстного меню событий угроз (такое меню показано на рисунке) можно отправить список на печать или включить/отключить отображение области описания событий.

В правой части строки под таблицей содержится счетчик событий угроз: <номер выбранного события>/<общее количество событий>.

Для настройки анализа записей и поиска событий угроз:

1. Загрузите записи журнала.
2. Переключите область отображения сведений в режим "угрозы" с помощью кнопки в верхней части области.
3. Нажмите кнопку "Запрос" в панели настройки вывода сведений (справа от области отображения сведений).

   На экране появится панель настройки параметров поиска угроз.



В списке представлены правила поиска событий угроз в загруженных записях журнала. По умолчанию список содержит предустановленные правила поиска общего характера. Эти правила поиска нельзя удалить из списка.

4. Сформируйте список правил поиска событий угроз. Управление правилами осуществляется с помощью кнопок под списком.

   Для формирования списка предусмотрены следующие возможности:

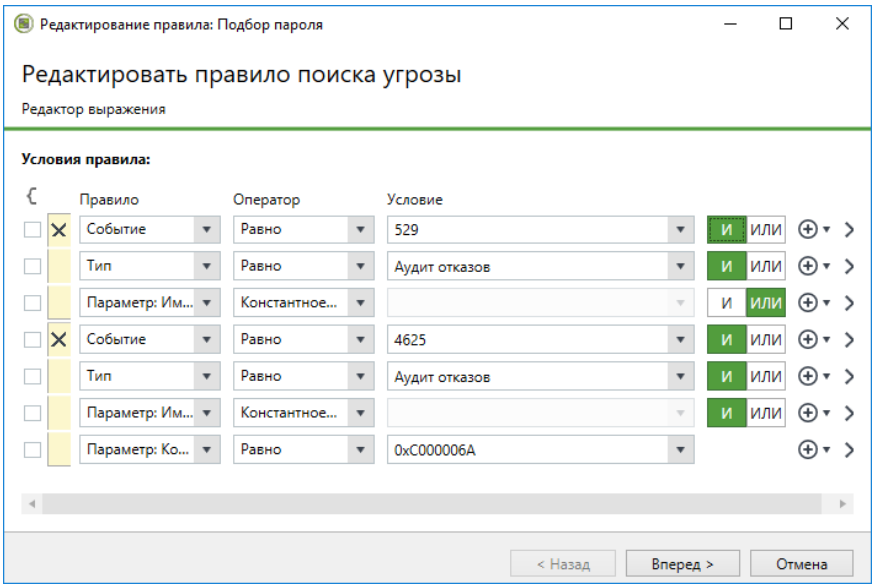
   - добавление и удаление правил поиска угроз (с помощью кнопок "Добавить правило поиска угрозы" и "Удалить правило угрозы");
   - копирование правил поиска угроз (с помощью кнопки "Копировать" создается копия выбранного правила, доступная для редактирования);
   - загрузка списка правил, сохраненного в файле (с помощью кнопки "Импорт правил угроз").

5. Настройте параметры поиска событий угроз. Настройка осуществляется отдельно для каждого правила с помощью мастера. При создании нового правила запуск мастера происходит автоматически. Чтобы настроить параметры имеющегося правила, выберите его в списке и нажмите кнопку "Редактировать правило угрозы" справа под списком правил или нажмите на нужное правило двойным щелчком мыши.

   Примечание. Стандартные правила системы Secret Net Studio не подлежат редактированию. Мастер запускается только для просмотра сведений о правиле.

   Диалоги мастера настройки параметров правила:

   - Диалог "Редактор выражения". Пример диалога представлен на рисунке ниже.



   Составьте список условий, которым должны удовлетворять записи для соответствия данному событию угрозы. Условия определяют содержимое полей в записях о событиях или параметров в описаниях событий. Для контроля содержимого поля или параметра в списке должно присутствовать выражение, задающее допустимые значения. Например, для поля "Тип" можно задать значение "Аудит отказов", чтобы при анализе рассматривались записи о событиях только этого типа.

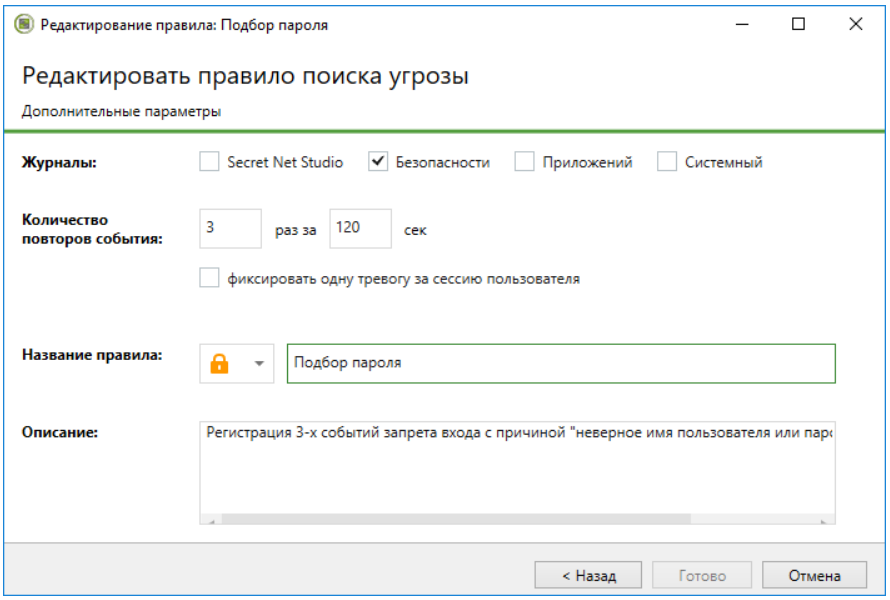
   Несколько выражений логически связываются между собой. Предусмотрены возможности использования логических операторов И, ИЛИ, а также группирования выражений. Например, можно задать обязательное совпадение заданных значений для полей "Тип", "Источник" и "Компьютер", чтобы при анализе не рассматривались записи, у которых хотя бы одно из значений в указанных полях не совпадает с заданным.

   Для формирования списка условий используйте следующие средства управления:

- средства группировки выражений (слева) — для объединения в группу отметьте нужные выражения и нажмите кнопку с фигурной скобкой, которая расположена над списком. Чтобы отменить группировку, нажмите кнопку в виде крестика в зоне группирования;
- средства определения условий для содержимого поля или параметра (в центре) — чтобы задать условие, укажите в раскрывающихся списках название нужного поля или параметра и его значения;
- средства выбора логической операции со следующим выражением или группой (кнопки "И/ИЛИ") — чтобы включить действие логического оператора, нажмите его кнопку (действующий оператор выделен зеленым цветом);
- средства добавления и удаления выражений (справа).

После формирования списка условий нажмите кнопку "Вперед" для перехода к следующему диалогу мастера.

- Диалог "Дополнительные параметры". Пример диалога представлен на рисунке ниже.



Отметьте журналы, записи которых будут рассматриваться при анализе на соответствие данному событию угрозы.

В группе полей "Количество повторов события" укажите параметры отслеживания нескольких записей, удовлетворяющих заданным условиям. Если требуется отследить повторяющиеся события, произошедшие в течение некоторого промежутка времени (например, для контроля попыток подбора пароля), укажите нужное количество повторов и интервал времени в секундах.

При необходимости можно включить режим сжатия в одно событие угрозы для случаев, когда при анализе выявляется несколько таких событий за время одного сеанса работы пользователя (к которому относятся записи). За счет этого сокращается список событий угроз. Данный режим следует использовать, если последовательность событий угроз в пределах одного сеанса работы не важна. Для включения режима сжатия установите отметку в поле "фиксировать одну тревогу за сессию пользователя".

В полях групп "Название правила" и "Описание" укажите пиктограмму для события угрозы, его название и дополнительные сведения.

Чтобы применить заданные параметры, нажмите кнопку "Готово" в диалоге мастера настройки параметров правила.

6. После настройки правил поиска событий угроз при необходимости сохраните список правил в файл для дальнейшего использования. Для этого нажмите кнопку "Экспорт правил угроз" слева под списком правил.
7. Отметьте в списке события угроз, поиск которых нужно выполнить, и нажмите кнопку "Поиск" в нижней части панели настройки параметров поиска угроз.

   После анализа загруженных записей появится список полученных событий угроз.

Примечание. Правила поиска угроз можно создавать непосредственно при работе с записями журналов. Для этого выделите нужные записи, вызовите контекстное меню и выберите команду "Добавить правило поиска угрозы". Далее настройте параметры правила в диалогах мастера настройки (аналогично вышеописанной процедуре).

Квитирование событий тревоги в журнале

Для квитирования в запросе с записями журнала событий тревоги:

1. Загрузите записи журнала событий тревоги из БД сервера безопасности (см. стр.**194**).
2. В списке записей журнала выделите записи о событиях, которые необходимо квитировать.
3. Вызовите контекстное меню одной из выбранных записей и выберите команду "Квитировать тревоги".

   На экране появится диалог для ввода текстового комментария.
4. Введите текстовый комментарий с описанием причин и принятых мер по факту возникновения событий и нажмите кнопку "Квитировать".

   В панели событий системы появится уведомление о квитировании событий тревоги, и признак квитирования будет присвоен выбранным записям.

Сортировка записей

Отображаемые записи сортируются по значениям, содержащимся в определенных колонках таблицы записей. Сортировка таблицы записей выполняется стандартными способами. Для сортировки по содержимому колонки наведите указатель на ее заголовок и нажмите левую кнопку мыши.

Поиск записей

Центр управления позволяет выполнить поиск записей, удовлетворяющих заданным параметрам или содержащих текстовую строку. Поиск осуществляется только среди отображаемых записей в текущем запросе.

Для поиска записей по заданным параметрам:

1. Загрузите записи журнала и настройте параметры запроса (см. стр.**194**).
2. Нажмите кнопку "Применить запрос локально".

   В таблице записей будут выделены все записи, удовлетворяющие заданным параметрам в запросе.

Цветовое оформление записей

Для наглядного представления информации предусмотрено цветовое оформление отображаемых записей (кроме журнала сервера безопасности).

При включенном режиме цветового оформления записи выделяются заданными цветами. Описание настройки параметров цветового оформления см. на стр.**284**.

Для включения режима цветового оформления:

1. Загрузите записи журнала (см. стр.**194**).

2. Вызовите контекстное меню любой записи и выберите команду "Раскраска событий".

   Записи будут выделены цветами, соответствующими характеристикам событий.

   Отключение режима цветового оформления выполняется аналогично.

Получение сведений о событиях из внешних баз знаний

При необходимости получения дополнительных сведений о зарегистрированном событии Центр управления позволяет выполнить запрос информации во внешних базах знаний, размещаемых в сети интернет. Внешние базы знаний могут содержать полезную информацию о причинах возникновения конкретных событий и рекомендации для пользователей. Предоставление информации во внешних базах знаний регулируется владельцами информационных ресурсов.

Получение информации во внешних базах знаний не предусмотрено для записей журнала сервера безопасности.

Для загрузки сведений компьютер должен иметь доступ в сеть интернет.

Для формирования запроса информации во внешней базе знаний:

1. Загрузите записи журнала (см. стр.**194**).
2. Вызовите контекстное меню записи о событии, по которому требуется получить информацию, раскройте подменю "Искать в базах знаний" и выберите соответствующую команду:
   - Microsoft Knowledge Base — для поиска в базе знаний на сайте http://www.microsoft.com;
   - Event ID Database — для поиска в базе знаний на сайте http://www.eventid.net.

   На экране появится окно веб-обозревателя, в котором будет загружена страница с результатами поиска в базе знаний.

Печать записей

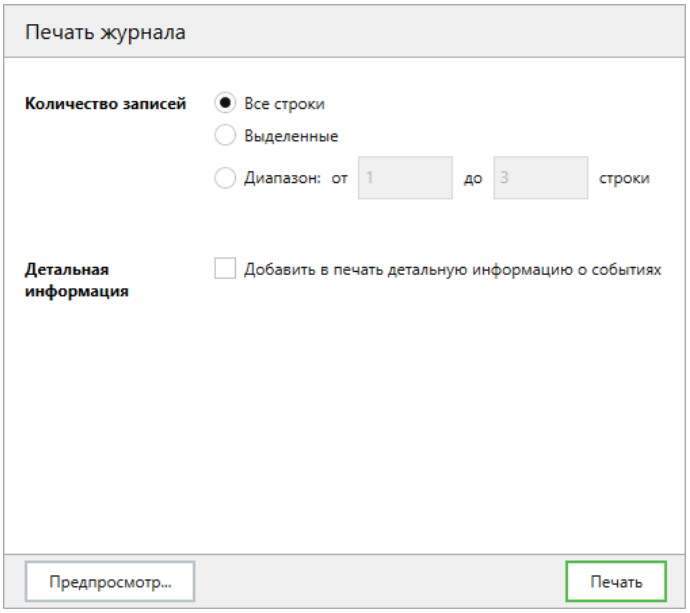
Центр управления позволяет отправлять на печать записи текущего запроса. Настройка параметров осуществляется в специальной панели настройки.

Возможность печати не предусмотрена для журнала сервера безопасности.

Для печати записей:

1. Загрузите записи журнала (см. стр.**194**).
2. Если требуется распечатать часть загруженных записей, выделите нужные записи в таблице.
3. Нажмите кнопку "Печать журнала" в панели настройки вывода сведений (справа от области отображения сведений).

   На экране появится панель настройки параметров печати.



4. Настройте параметры печати.

Группа полей "Количество записей"
Определяет, какие записи будут распечатаны: • "Все строки" — выполняется печать записей, отображаемых в соответствии с текущими параметрами фильтрации; • "Выделенные" — выполняется печать только тех записей, которые выделены в таблице; • "Диапазон" — позволяет задать диапазон записей для печати по порядку их следования в таблице (в соответствии с текущими параметрами сортировки). Границы диапазона определяются в полях "от" и "до". Первая и последняя записи диапазона также будут распечатаны
Поле "Детальная информация"
Если установлена отметка, будет распечатано содержимое полей с детальным описанием событий

5. Чтобы открыть окно предварительного просмотра страниц, нажмите кнопку "Предпросмотр" в нижней части панели настройки параметров печати. После просмотра запустите процесс с помощью стандартной кнопки отправки на печать на панели инструментов окна предварительного просмотра.

Примечание. Запуск процесса печати можно выполнить без открытия окна предварительного просмотра. Для этого нажмите кнопку "Печать" в нижней части панели настройки параметров печати.

На экране появится диалог ОС Windows для выбора принтера и настройки общих параметров печати.

6. Выберите принтер и нажмите кнопку "Печать".

Экспорт записей

Центр управления позволяет экспортировать (сохранять) в файлы записи текущего запроса. Настройка параметров осуществляется в специальной панели настройки.

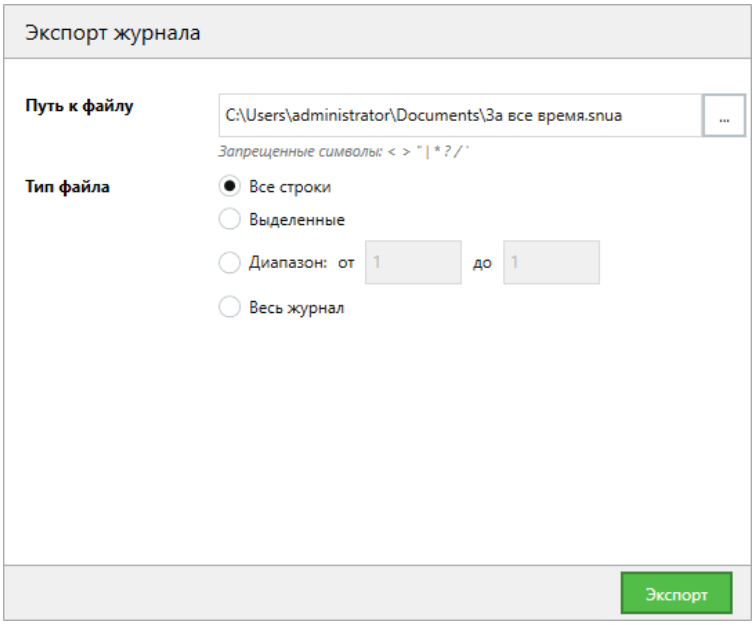
Экспорт осуществляется в файлы специальных форматов:

- записи журнала событий тревоги — экспортируются в файлы формата *.snua;
- записи журнала станций — экспортируются в файлы формата *.snlog;
- записи журнала сервера безопасности — экспортируются в файлы формата *.snsrv.

Для экспорта записей:

1. Загрузите записи журнала (см. стр.**194**).
2. Если требуется экспортировать часть загруженных записей, выделите нужные записи в таблице.
3. Нажмите кнопку "Экспорт журнала" в панели настройки вывода сведений (справа от области отображения сведений).

   На экране появится панель настройки параметров экспорта.



4. Чтобы указать файл для сохранения, нажмите кнопку в правой части поля "Путь к файлу" и выберите размещение в диалоге сохранения файла ОС Windows.
5. Настройте параметры экспорта.

Группа полей "Тип файла"
Определяет, какие записи будут экспортированы: • "Все строки" — выполняется экспорт записей, отображаемых в соответствии с текущими параметрами фильтрации; • "Выделенные" — выполняется экспорт только тех записей, которые выделены в таблице; • "Диапазон" — позволяет задать диапазон записей для экспорта по порядку их следования в таблице (в соответствии с текущими параметрами сортировки). Границы диапазона определяются в полях "от" и "до". Первая и последняя записи диапазона также будут экспортированы; • "Весь журнал" — выполняется экспорт всех записей, загруженных в запрос (в том числе тех, которые не удовлетворяют текущим параметрам фильтрации)

6. Нажмите кнопку "Экспорт".

Архивирование централизованных журналов по команде администратора

Архивирование централизованных журналов, хранящихся в БД сервера безопасности, выполняется регулярно в соответствии с заданными параметрами для сервера безопасности (см. стр.**150**).

При работе с Центром управления можно выполнить запуск процесса внеочередного архивирования централизованных журналов. Команда архивирования применяется к серверу безопасности, с которым установлено соединение.

Для запуска процесса архивирования журналов:

1. В диаграмме управления или в списке объектов вызовите контекстное меню сервера безопасности, раскройте подменю "Архивирование" и выберите команду "Создать архив журналов".

   На экране появится диалог для настройки параметров архивирования.

2. Настройте параметры архивирования, представленные ниже. После настройки нажмите кнопку "Архивировать".

Поля "События до"
Поля определяют границу интервала времени. В архив будут помещены записи, которые были зарегистрированы до указанного момента времени
Поле "Журналы"
Поле определяет типы журналов, записи которых должны архивироваться
Поле "Описание"
Введите в этом поле краткое описание создаваемого архива

Глава 17
Дополнительные возможности локального администрирования

Редактирование учетной информации компьютера

В учетной информации компьютера могут быть указаны следующие сведения:

- название подразделения, в котором используется компьютер;
- наименование автоматизированной системы предприятия;
- место расположения компьютера;
- номер системного блока.

Ввод учетной информации можно выполнить при установке клиентского ПО системы Secret Net Studio или позже. Возможности редактирования учетной информации предоставляются в Центре управления (см. стр. 174), а также в диалоговом окне "Управление Secret Net Studio".

Для редактирования учетной информации в диалоговом окне "Управление Secret Net Studio":

1. В Панели управления Windows выберите ярлык "Управление Secret Net Studio".

   Если на компьютере включена функция "Контроль административных привилегий", на экране появится диалоговое окно ввода PIN администратора.
2. В поле "PIN администратора" введите PIN администратора и нажмите кнопку "ОК".

   На экране появится диалоговое окно "Управление Secret Net Studio".
3. Перейдите к диалогу "Учетная информация".
4. Введите сведения о компьютере в соответствующих полях.
5. Нажмите кнопку "Применить" или "ОК".

Локальное оповещение о событиях тревоги

События тревоги считаются события, которые регистрируются в журнале Secret Net Studio или штатном журнале безопасности ОС и имеют тип "Аудит отказов" или "Ошибки". При возникновении на компьютере таких событий система защиты может локально оповещать об этом текущего пользователя компьютера.

Режим локального оповещения о событиях тревоги можно включать и отключать для всех пользователей компьютера (компьютеров) или предоставить пользователям возможность управлять режимом самостоятельно.

Ниже приводится описание процедуры централизованной настройки на рабочем месте администратора в Центре управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для управления режимом локального оповещения о событиях тревоги:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Оповещение о тревогах".

3. Для параметра "Локальное оповещение о тревогах" укажите режим действия или выберите значение "Определяется пользователем".

Примечание. Переключение режима локального оповещения пользователем осуществляется с помощью команды "Уведомления о тревогах" в контекстном меню пиктограммы Secret Net Studio, находящейся в панели задач Windows.

4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Локальное управление лицензиями

В системе Secret Net Studio действуют лицензионные ограничения на использование ряда подсистем, реализующих применение механизмов защиты. Управление лицензиями осуществляется с помощью специальных файлов.

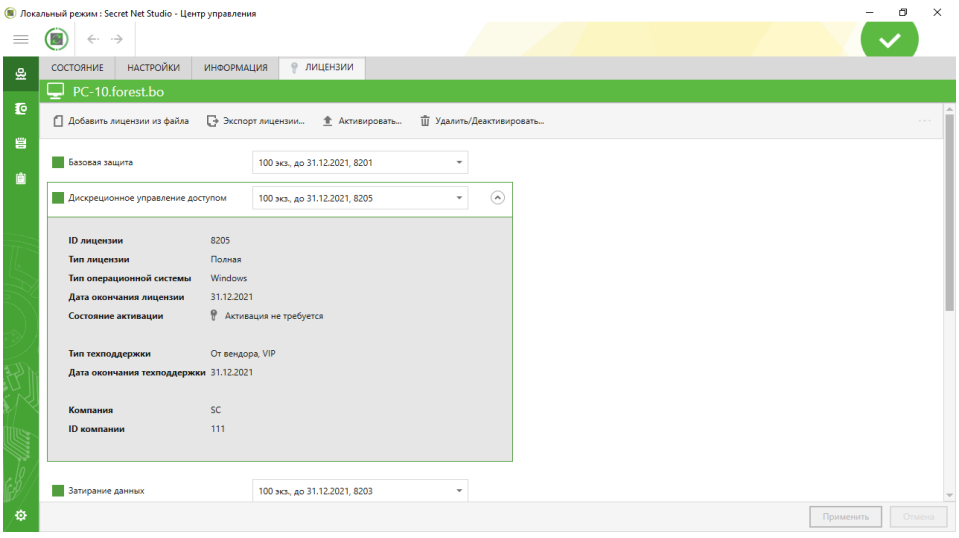
Для клиентов Secret Net Studio в сетевом режиме работы операции с лицензиями осуществляются на сервере безопасности. При подключении клиента к серверу происходит проверка лицензионных условий, и соответствующая клиентская лицензия загружается с сервера безопасности в локальное хранилище клиента. Управление лицензиями на сервере безопасности выполняется в Центре управления в централизованном режиме работы.

Также в системе предусмотрено локальное управление лицензиями на защищаемых компьютерах. Локальное управление может потребоваться для клиента в автономном режиме работы, а также и в сетевом режиме, если подключение к серверу безопасности невозможно длительное время.

Внимание! Если лицензия хотя бы на одну работающую подсистему не активирована, отсутствует или ее срок действия истек, то клиентское ПО переходит в ограниченный режим работы, при котором невозможно редактировать настройки системы защиты, а также запускать большую часть защитных утилит.

Для локальной регистрации лицензий:

1. В Локальном центре управления откройте панель "Компьютер" и перейдите на вкладку "Лицензии".



На вкладке представлен список лицензируемых подсистем и сведения о текущем состоянии лицензий. Активированные подсистемы (с действующими лицензиями) имеют отметки слева от названий. Чтобы отобразить подробные сведения о лицензии на подсистему, наведите на строку с названием подсистемы и нажмите кнопку, которая появляется в выделенной строке справа.

2. При наличии файла с лицензиями, которые нужно зарегистрировать, нажмите кнопку "Добавить лицензии из файла", которая расположена над списком лицензируемых подсистем. В появившемся диалоге выбора файла выберите нужный файл с лицензиями.

   После обработки данных список лицензий будет обновлен.

3. Для управления активацией подсистем (включение и отключение действия лицензий) используйте элементы управления, расположенные слева от названий подсистем. При отключении действия лицензии поле со сведениями о лицензии для подсистемы становится пустым и ниже выводится сообщение об удалении лицензии.
4. Для сохранения текущей конфигурации лицензий нажмите кнопку "Применить" в нижней части вкладки.

Для локального экспорта лицензий:

1. В Локальном центре управления откройте панель "Компьютер" и перейдите на вкладку "Лицензии".
2. Нажмите кнопку "Экспорт лицензии", которая расположена над списком лицензируемых подсистем. В появившемся диалоге укажите путь для экспорта файла с лицензиями.

Для локальной активации лицензий:

1. В Локальном центре управления откройте панель "Компьютер" и перейдите на вкладку "Лицензии".
2. Нажмите кнопку "Активировать", которая расположена над списком лицензируемых подсистем. В появившемся диалоге выбора файла выберите путь для экспорта файла с лицензиями, выберите подсистемы, для которых нужно активировать лицензии, и нажмите кнопку "Вперед".
3. Выберите вариант активации лицензий и нажмите кнопку "Применить".
4. При выборе активации через личный кабинет загрузите файл запроса на страницу активации в личном кабинете, дождитесь активации лицензии и скачайте файл с активированными лицензиями.

   Нажмите кнопку "Добавить лицензии из файла", которая расположена над списком лицензируемых подсистем. В появившемся диалоге выбора файла выберите файл с активированными лицензиями.

Для локального удаления лицензий:

1. В Локальном центре управления откройте панель "Компьютер" и перейдите на вкладку "Лицензии".
2. Нажмите кнопку "Удалить/Деактивировать", которая расположена над списком лицензируемых подсистем. В появившемся диалоге выберите лицензии, которые необходимо удалить с клиента, и нажмите кнопку "Применить".

Для локальной деактивации лицензий:

1. В Локальном центре управления откройте панель "Компьютер" и перейдите на вкладку "Лицензии".
2. Нажмите кнопку "Удалить/Деактивировать", которая расположена над списком лицензируемых подсистем. В появившемся диалоге выберите лицензии, которые необходимо удалить с клиента.
3. Поставьте отметку в поле "Деактивировать лицензии при удалении" и нажмите кнопку "Вперед".
4. Выберите вариант деактивации лицензий и нажмите кнопку "Применить".

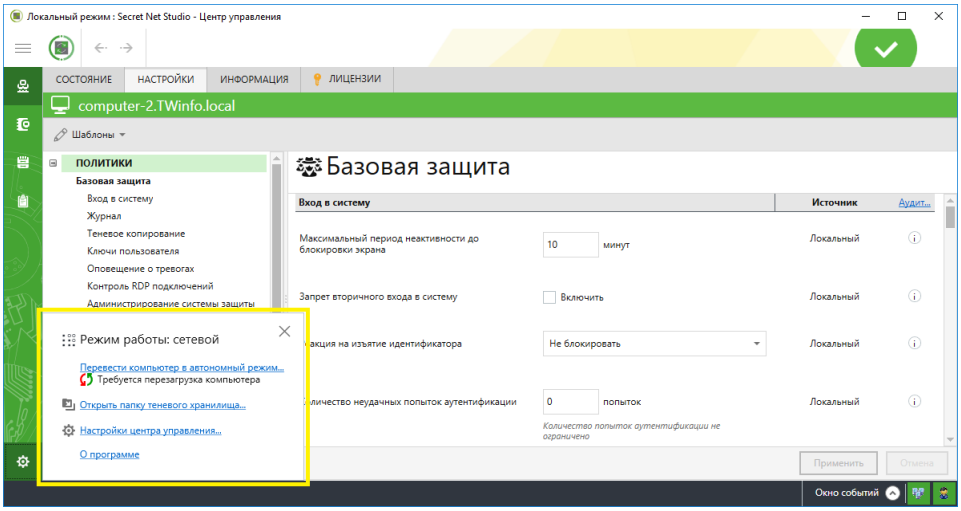
Внимание! Для деактивации лицензии на подсистему "Базовая защита" необходимо предварительно деактивировать лицензии на все остальные подсистемы.

Изменение режима работы клиента

Клиент системы Secret Net Studio может функционировать в автономном и сетевом режимах. Текущий режим работы клиента отображается в Локальном центре управления. Переключение между режимами можно выполнить в Локальном центре управления и с использованием командной строки.

Для просмотра информации о текущем режиме работы клиента:

- В Локальном центре управления в нижней части панели навигации нажмите кнопку "Настройки". На экране появится панель вызова средств настройки:



  В верхней части панели вызова средств настройки отобразится режим работы клиента:

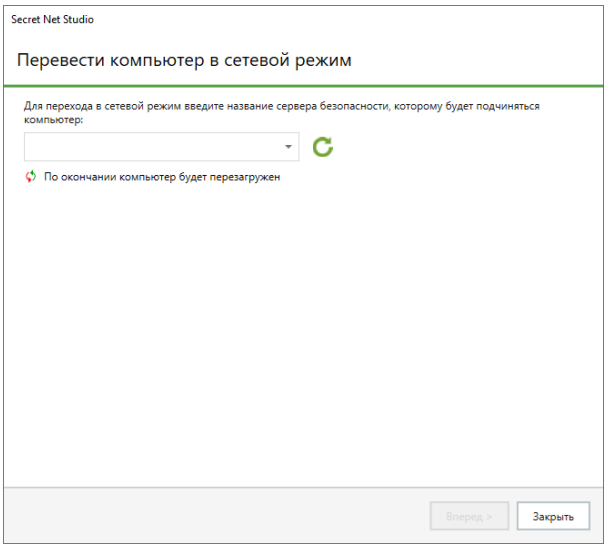
  - "Режим работы: автономный" — при функционировании клиента в автономном режиме;
  - "Режим работы: сетевой" — при функционировании клиента в сетевом режиме;
  - "Режим работы: идет определение режима" — при выполнении процесса определения режима;
  - "Режим работы: не определен" — при возникновении ошибок в процессе определения режима.

  Пояснение. Если режим работы клиента не определен, перезагрузите компьютер.

Для переключения клиента из автономного режима в сетевой:

1. В Локальном центре управления в нижней части панели навигации нажмите кнопку "Настройки" и выберите команду "Перевести компьютер в сетевой режим...".

   На экране появится окно с запросом учетных данных сервера безопасности.



2. Укажите наименование сервера безопасности, которому должен подчиняться клиент, одним из следующих способов:

- нажмите кнопку для поиска доступных серверов безопасности и выберите необходимый сервер из списка найденных;
- введите наименование сервера безопасности самостоятельно.

3. Нажмите кнопку "Вперед".

Пояснение. Для отмены перехода в сетевой режим нажмите кнопку "Закрыть".

Начнется процесс проверки учетных данных сервера безопасности. Возможны следующие ошибки:

- наименование сервера безопасности введено неверно. В этом случае система выдаст сообщение об ошибке. Нажмите "Закрыть" и повторите процедуру;

  Пояснение. Если наименование сервера безопасности введено неверно, в журнале будет зарегистрировано событие "Ошибка. Входной параметр имеет нулевое значение. Сервер не найден".

- недостаточно прав для подчинения клиента серверу безопасности. В этом случае система выдаст сообщение об ошибке. Нажмите "ОК" и повторите процедуру с правами администратора домена безопасности.

При успешном завершении проверки учетных данных сервера безопасности.

4. Выберите лицензии на сервере безопасности или на данном компьютере и нажмите кнопку "Вперед".
5. Выберите вариант деактивации лицензий, использовавшихся в автономном режиме работы клиента, и нажмите кнопку "Переключить".

Внимание! Для использования данных лицензий на другом автономном клиенте их необходимо деактивировать.

Начнется процесс настройки клиента для работы в сетевом режиме.

Пояснение. При переводе клиента из автономного режима работы в сетевой система Secret Net Studio выполняет следующие действия:
- создает учетную запись клиента в структуре централизованного управления;
- создает запись о сервере безопасности в реестре клиента;
- вводит ключ активации лицензии клиента;
- подключает клиент к домену безопасности;
- переводит механизмы защиты клиента в сетевой режим работы.

При успешном завершении процесса настройки появится окно с сообщением о переводе клиента в сетевой режим и необходимости перезагрузить компьютер.

6. Нажмите кнопку "Перезагрузить".

Клиент будет переведен в сетевой режим. Выполнится проверка лицензии клиента. При возникновении ошибки лицензирования система выдаст соответствующее сообщение. В этом случае скорректируйте лицензии в программе управления, запущенной в централизованном режиме.

Пояснение. Для переключения клиента из автономного режима в сетевой в командной строке перейдите в каталог установки клиента и выполните команду:

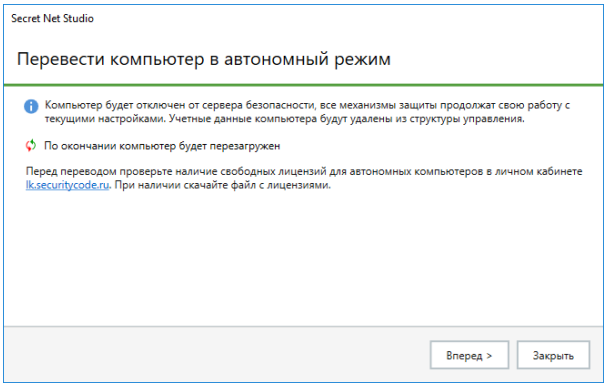
```
medusa.exe /switchmode=network /omserverName=<SERVERNAME>
/omserverPort=<PORT>
```

где:
- <SERVERNAME> — имя сервера безопасности, которому должен подчиняться клиент;
- <PORT> — порт сервера безопасности. Если параметр не задан, будет использоваться порт 443.

Для переключения клиента из сетевого режима в автономный:

1. В Локальном центре управления в нижней части панели навигации нажмите кнопку "Настройки" и выберите команду "Перевести компьютер в автономный режим...".

   На экране появится предупреждение:



Пояснение. При переводе клиента из сетевого режима работы в автономный система Secret Net Studio выполняет следующие действия:

- удаляет учетные данные о клиенте из структуры централизованного управления;
- переводит механизмы защиты клиента в автономный режим работы с сохранением текущих настроек, но без сохранения лицензии;
- удаляет учетные данные сервера безопасности из локальной БД клиента.

2. Нажмите кнопку "Вперед".

Пояснение. Для отмены перехода в автономный режим нажмите кнопку "Закрыть".

Выберите файл лицензий для использования клиентом в автономном режиме и нажмите кнопку "Переключить".

Внимание! Переключение клиента в автономный режим возможно с неактивированными лицензиями либо без лицензий. В таком случае клиент будет функционировать в ограниченном режиме работы, при котором невозможно редактировать настройки системы защиты, а также запускать большую часть защитных утилит. Лицензии можно будет добавить и активировать позже через Локальный центр управления.

Начнется процесс настройки клиента для работы в автономном режиме.

При успешном завершении процесса настройки появится окно с сообщением о переводе клиента в автономный режим и необходимости перезагрузить компьютер.

Пояснение. При переходе в автономный режим учетные данные о клиенте могут не удалиться из структуры управления автоматически. В этом случае система выдаст соответствующее предупреждение. После перевода клиента в автономный режим удалите учетные данные самостоятельно.

3. Нажмите кнопку "Перезагрузить".

Клиент будет переведен в автономный режим.

Пояснение. Для переключения клиента из сетевого режима в автономный в командной строке перейдите в каталог установки клиента и выполните команду:

```
medusa.exe /switchmode=standalone
```

Приложение

Правила приемки и методы контроля

Приемка Secret Net Studio проводится в следующем объеме и последовательности:

1. Проверка комплектности и маркировки изделия.
2. Проверка контрольных сумм дистрибутивного комплекта ПО изделия.

Проверка комплектности и маркировки

Комплектность изделия проверяется внешним осмотром путем сравнения с данными, приведенными в формуляре изделия.

Проверка считается успешной, если комплектность изделия соответствует требованиям, приведенным в формуляре изделия.

Сертифицированные образцы изделия должны маркироваться идентификатором РОСС RU.01.XXXXX.XXXXXX, где первая группа знаков РОСС RU.01 указывает на систему сертификации ФСТЭК России, вторая группа знаков (числа 00001–99999) – номер сертификата, третья группа (числа 000001– 999999) – серийный номер сертифицированного образца. Идентификатор сертифицированного СЗИ указывается в формуляре изделия в разделе "Свидетельство об изготовлении, упаковке, маркировке и приемке", на коробке для компакт-диска и формуляра и упаковочной коробке комплекта СЗИ. Идентификатор также заносится в базу данных фирмы-изготовителя.

Требования к маркировке:

1. При маркировке лицевой стороны установочного компакт- диска указываются:
- наименование изделия;
- наименование фирмы-изготовителя;
- номер сертификата.
2. При маркировке коробки для компакт-диска и формуляра указываются:
- наименование изделия;
- реквизиты фирмы-изготовителя;
- заводской номер;
- идентификатор сертифицированного СЗИ.
3. При маркировке упаковочной коробки комплекта СЗИ указываются:
- штрихкод;
- заводской номер;
- идентификатор сертифицированного СЗИ.

Проверка считается успешной, если маркировка соответствует требованиям, приведенным выше.

Проверка контрольных сумм дистрибутивного комплекта ПО

Проверка соответствия дистрибутивного носителя эталону проводится путем расчета контрольных сумм соответствующих файлов и их сравнения с контрольными суммами, указанными в приложении 1 к формуляру изделия.

Проверка считается успешной, если все контрольные суммы проверяемых файлов совпадают с эталонными контрольными суммами, указанными в приложении 1 к формуляру изделия.

Необходимые права для установки и управления

Система Secret Net Studio обеспечивает возможности входа и выполнения операций для любых зарегистрированных пользователей в рамках полномочий, которыми они обладают в ОС и механизмах защиты. Для установки компонентов Secret Net Studio и управления работой системы пользователи дополнительно должны обладать определенными административными полномочиями. Состав необходимых прав и привилегий для администрирования зависит от выполняемых операций.

Для автономного режима функционирования установка ПО клиента Secret Net Studio и все функции управления доступны пользователям, входящим в локальную группу администраторов компьютера. Некоторые функции (например, управление журналом Secret Net Studio) могут быть переданы другим пользователям путем предоставления соответствующих привилегий.

Ниже в данном разделе приводится список основных операций при использовании системы Secret Net Studio в сетевом режиме функционирования. Для каждой операции указаны учетные записи, для которых доступно выполнение действий. Используются следующие условные обозначения учетных записей:

- **Администраторы леса доменов безопасности** — пользователи, включенные в группу администраторов леса доменов безопасности Secret Net Studio (группа указывается при установке сервера безопасности, если выбран вариант создания домена в новом лесу доменов безопасности — то есть устанавливается первый СБ в лесу доменов безопасности);
- **Администраторы домена безопасности** — пользователи, включенные в группу администраторов домена безопасности Secret Net Studio (группа указывается при установке сервера безопасности, если выбран вариант создания нового домена безопасности — то есть устанавливается первый СБ в домене безопасности);
- **Администраторы** — пользователи, включенные в стандартную локальную группу администраторов компьютера (Администраторы);
- **Привилегия <*название_привилегии*>** — пользователи, которым назначена указанная привилегия.

Установка и удаление компонентов

Основные операции при установке или удалении компонентов системы Secret Net Studio представлены в следующих таблицах.

Табл.1 Установка и удаление сервера безопасности

Операция	Учетные записи с правами на выполнение
Создание групп пользователей для администраторов леса домена безопасности и администраторов домена безопасности	Пользователи с правами для создания групп в домене AD и для включения пользователей в группы
Установка с созданием домена в новом лесу доменов безопасности	• Administrators (доменный пользователь). • Администраторы домена безопасности
Установка с созданием нового домена безопасности в существующем лесу	• Administrators. • Администраторы леса доменов безопасности. • Администраторы домена безопасности

Операция	Учетные записи с правами на выполнение
Установка с добавлением сервера в существующий домен безопасности	• Administrators. • Администраторы леса доменов безопасности. • Администраторы домена безопасности
Удаление в штатном режиме: с одновременным удалением сервера из структуры ОУ	• Administrators. • Администраторы домена безопасности
Удаление в нештатном режиме: без корректировки структуры ОУ[1]	Administrators

[1]Операция, в результате которой на компьютере будет удалено ПО сервера безопасности, но информация о сервере останется в структуре ОУ. Для удаления сервера из структуры можно использовать Центр управления (см. стр.220). Данный вариант возможен, если в системе присутствует хотя бы один сервер безопасности, доступный для подключения программы. При нештатном удалении последнего сервера леса доменов данные леса доменов безопасности уничтожаются при удалении ПО сервера.

Табл.2 Установка и удаление клиента

Операция	Учетные записи с правами на выполнение
Установка с подключением к серверу безопасности	• Administrators. • Администраторы домена безопасности
Установка без подключения к серверу безопасности[1]	Administrators
Удаление с одновременным удалением клиента из структуры ОУ	• Administrators. • Администраторы домена безопасности
Удаление без корректировки структуры ОУ[2]	Administrators

[1]Операция, в результате которой на компьютере будет установлено ПО клиента, но клиент не будет связан с сервером безопасности в структуре ОУ. Для добавления сопоставленного клиенту агента в структуру и подчинения его серверу безопасности можно использовать Центр управления (см. стр.220).

[2]Операция, в результате которой на компьютере будет удалено ПО клиента, но информация о клиенте останется в структуре ОУ. Для удаления сопоставленного клиенту агента из структуры ОУ можно использовать Центр управления (см. стр.220).

Табл.3 Установка и удаление Центра управления

Операция	Учетные записи с правами на выполнение
Установка	Administrators
Удаление	Administrators

Настройка механизмов и управление параметрами объектов

Основные операции при настройке механизмов защиты системы Secret Net Studio и изменении параметров объектов (пользователей, компьютеров) представлены в следующей таблице.

Табл.4 Настройка механизмов и управление параметрами объектов

Операция	Учетные записи с правами на выполнение
Создание и удаление групп пользователей	• Пользователи с правами для создания и удаления учетных записей в домене AD. • Administrators
Создание и удаление пользователей	• Пользователи с правами для создания и удаления учетных записей в домене AD. • Администраторы домена безопасности Administrators
Управление параметрами пользователей, присвоение и настройка идентификаторов	• Администраторы домена безопасности. • Administrators
Формирование списка компьютеров для входа в ПАК "Соболь"	Администраторы домена безопасности
Управление ключами ЦУ ПАК "Соболь"	• Администраторы домена безопасности. • Administrators
Локальное управление параметрами компьютера: редактирование учетной информации, подключение ПАК "Соболь"	• Администраторы домена безопасности. • Administrators
Управление параметрами КЦ-ЗПС	• Администраторы домена безопасности. • Administrators

Работа с Центром управления в централизованном режиме

Основные операции в Центре управления системы Secret Net Studio представлены в следующей таблице.

Табл.5 Использование Центра управления

Операция	Учетные записи с правами на выполнение
Подключение к серверу безопасности и просмотр информации	Привилегия "Просмотр информации" для сервера подключения
Конфигурирование агентов (добавление в структуру ОУ, удаление, подчинение и настройка параметров в режиме конфигурирования)	Администраторы домена безопасности
Конфигурирование серверов безопасности (добавление в структуру ОУ, удаление, подчинение и настройка параметров в режиме конфигурирования)	Администраторы домена безопасности
Корректировка структуры ОУ после нештатного удаления сервера безопасности: удаление сервера при подключении к СБ в другом домене в том же лесу[1]	• Администраторы домена безопасности (в домене сервера подключения). • Администраторы домена безопасности (в домене удаленного сервера)

Операция	Учетные записи с правами на выполнение
Настройка параметров групповых политик доменов и организационных подразделений	• Администраторы домена безопасности. • Привилегия "Редактирование политик" для сервера подключения. Для управления группой параметров "Администрирование системы защиты" дополнительно требуется привилегия "Администрирование системы защиты" на сервере подключения
Удаленная настройка локальных параметров Secret Net Studio: параметры локальной политики безопасности, аппаратная конфигурация, состояние защитных механизмов	• Привилегии "Редактирование политик". • "Выполнение оперативных команд" для сервера подключения. Для управления группой параметров "Администрирование системы защиты" дополнительно требуется привилегия "Администрирование системы защиты" на сервере подключения
Выполнение команд оперативного управления компьютерами: блокировка, перезагрузка, обновление политик	Привилегия "Выполнение оперативных команд" для сервера подключения
Запуск процесса внеочередного сбора журналов с защищаемых компьютеров	Привилегия "Сбор журналов по команде" для сервера подключения
Запуск процесса внеочередного архивирования журналов в БД сервера безопасности	Привилегия "Архивирование/восстановление журналов" для сервера подключения
Квитирование событий тревоги (подтверждение приема информации)	Привилегия "Квитирование сообщений о тревогах" для сервера подключения

[1] Операция выполняется, если ПО сервера безопасности было удалено в нештатном режиме без корректировки структуры ОУ (см. стр. **218**) и при этом для подключения программы доступен СБ в другом домене того же леса. Если можно выполнить подключение к серверу в том же домене, для удаления объекта из структуры достаточно полномочий, требуемых при конфигурировании серверов безопасности (см. выше).

Оценка размера БД для сервера безопасности

Для установки и функционирования сервера безопасности в системе должен быть установлен сервер СУБД. Чтобы обеспечить производительность и необходимое время хранения накопленных данных, предварительно следует оценить размер будущей базы данных и нужный объем дискового пространства на компьютере сервера СУБД. Исходя из результатов оценки принимается решение о выборе редакции СУБД (свободно распространяемые редакции имеют ограничение на размер базы данных) и аппаратной конфигурации компьютера.

Основные критерии для оценки:

- Поток событий — количество регистрируемых событий в течение определенного периода времени. Базовое значение — поток событий в секунду (Events Per Second, EPS). Суммируются события, регистрируемые в штатных журналах ОС и в журнале Secret Net Studio. Нужно учитывать, что на поток событий существенно влияют роль компьютера в системе (сервер, рабочая станция), а также заданные параметры функционирования и регистрации в подсистемах.
- Размер записей о событиях — объем сохраняемой информации о событиях в записях журналов. Зависит от заполнения полей в записях различными данными: описания событий, сведения об источниках и объектах, другие данные. Размер записи о событии может варьироваться в широких пределах, поэтому целесообразно оценивать среднее значение.

- Срок хранения журналов — определяет время хранения журналов в базе данных и в архивах. Журналы должны быть доступны для оперативного получения сведений об инцидентах и нарушениях политики безопасности, для проведения аудита и определения потенциальных угроз. Срок хранения журналов должен быть достаточным, чтобы осуществлять ретроспективный анализ состояния системы.

  Примечание. Для обеспечения работоспособности сервера СУБД и минимизации издержек на поддержку инфраструктуры необходимо регулярно выполнять архивацию журналов. По умолчанию архивы сохраняются в подкаталоге \Archive каталога установки сервера безопасности. При необходимости архив можно загрузить в базу данных для анализа содержимого хранящихся в нем журналов.

Ниже рассматривается пример расчета для типовой АС класса защищенности 1Г, состоящей из одного сервера безопасности и 100 клиентских компьютеров. Для сервера безопасности используется компьютер под управлением ОС Windows Server 2012, для клиентов — ОС Windows 8.

Табл.6 Поток событий и средний размер записей на сервере безопасности

Журналы	Среднее количество событий в секунду (EPS)	Средний размер записи (байт)
Штатные журналы ОС	3	1000
Журнал Secret Net Studio	0,05	800

Табл.7 Поток событий и средний размер записей на клиенте

Журналы	Среднее количество событий в секунду (EPS)	Средний размер записи (байт)
Штатные журналы ОС	1	1000
Журнал Secret Net Studio	0,05	800

Табл.8 Объем журналов

Журналы	Количество событий в день	Заполнение БД за день (Мбайт)[1]	Объем журналов в БД за 7 дней (Мбайт)[2]	Объем журналов в архиве за 1 год (Мбайт)[3]
Сервер безопасности, 1 компьютер				
Штатные журналы ОС	259 200	259,2	1 814,4	2 365
Журнал Secret Net Studio	4 320	3,5	24,2	31,5
Клиент Secret Net Studio, 100 компьютеров				
Штатные журналы ОС	8 640 000	8 640	60 480	78 840
Журнал Secret Net Studio	432 000	345,6	2 419,2	3 153
Всего для сервера безопасности и клиентов				
		9 248,3	64 737,8	84 390

[1] Указан размер таблиц, содержащих журналы событий. Общий размер базы данных зависит также от размеров журнала транзакций и проводимых операций по оптимизации, сжатию базы.

[2] При использовании СУБД MS SQL Express 2012 (в данной редакции действует ограничение на размер базы в 10 Гбайт) следует уменьшить число источников данных. Для этого можно сократить количество подчиненных компьютеров до 10 либо в параметрах передачи локальных журналов отключить сбор штатных журналов ОС.

[3] С учетом сжатия архива с коэффициентом 40:1.

Внимание! Чтобы не увеличивался общий объем базы и сохранялась производительность, регулярно выполняйте операции по архивированию журналов СУБД и оптимизации структуры базы для удаления пустых страниц и дефрагментации записей в базе. В случае переполнения базы (при использовании свободно распространяемых СУБД, имеющих ограничения по размеру базы) необходимо выполнить действия по очистке базы данных, описанные в документе с комментариями к выпущенной версии (Release Notes).

Рекомендации по настройке для соответствия требованиям о защите информации

В разделе приведены значения параметров безопасности Secret Net Studio – C, которые рекомендуется установить в целях соответствия информационной системы требованиям о защите информации, предъявляемым к информационным системам различных типов и классов/уровней защищенности.

Настроить параметры безопасности можно вручную или с использованием стандартных шаблонов параметров безопасности для информационных систем различных типов и классов/уровней защищенности (см. стр.144).

Примечание. Стандартные шаблоны параметров безопасности не поддерживаются клиентами Secret Net LSP.

Автоматизированные системы

При определенных вариантах настройки система Secret Net Studio обеспечивает соответствие требованиям для следующих классов защищенности АС согласно классификации документа "Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации":

- АС первой группы:
  - 1Б;
  - 1В;
  - 1Г;
  - 1Д.
- АС второй группы:
  - 2А;
  - 2Б.
- АС третьей группы:
  - 3А;
  - 3Б.

Использование средств защиты загрузки

В АС должны применяться средства, исключающие доступ пользователя к ресурсам компьютера в обход механизмов системы защиты. Для систем любого класса до 1Б включительно в качестве такого средства может использоваться изделие "Программно-аппаратный комплекс "Соболь".

При использовании Secret Net Studio на виртуальных машинах в виртуальной инфраструктуре на базе продуктов VMware Infrastructure или VMware vSphere в качестве средства доверенной загрузки виртуальных машин может применяться изделие "Средство защиты информации vGate R2" или "Средство защиты информации vGate-S R2", совместимое с версией используемого продукта.

Вместо вышеперечисленных средств или совместно с любым из них может быть разработан и внедрен комплекс организационно-технических мероприятий, обеспечивающих невозможность доступа пользователей к информации на дисках компьютера в обход механизмов системы Secret Net Studio.

Параметры политик Secret Net Studio

Для соответствия классам защищенности АС должны быть настроены параметры политик, перечисленные в следующей таблице. Настройка выполняется в Центре управления на вкладке "Настройки", раздел "Политики".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;

- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.9 Параметры политик

Параметр	Классы защищенности АС		
	1Б, 1В, 1Г, 1Д	**2А, 2Б**	**3А, 3Б**
Группа "Вход в систему"			
Максимальный период неактивности до блокировки экрана	все: Не более 10 (реком.)	все: Не более 10 (реком.)	все: Не более 10 (реком.)
Запрет вторичного входа в систему	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Режим идентификации пользователя	все: Смешанный (реком.)	все: Смешанный (реком.)	все: Смешанный (реком.)
Режим аутентификации пользователя	все: Усиленная аутентификация по паролю (обяз.)	все: Усиленная аутентификация по паролю (обяз.)	все: Усиленная аутентификация по паролю (обяз.)
Режим аутентификации пользователя: Регистрировать неверные аутентифика-ционные данные	1Б,1В,1Г: Да (обяз.) 1Д: –	все: Да (обяз.)	3А: Да (обяз.) 3Б: –
Парольная политика	все: Задать свои значения (обяз.)	все: Задать свои значения (обяз.)	все: Задать свои значения (обяз.)
Минимальная длина пароля	1Б: Не менее 8 символов (обяз.) 1В,1Г,1Д: Не менее 6 символов (обяз.)	все: Не менее 6 символов (обяз.)	все: Не менее 6 символов (обяз.)
Срок действия пароля	1Б: Не более 90 дней (обяз.) 1В,1Г,1Д: Не более 180 дней (обяз.)	все: Не более 180 дней (обяз.)	все: Не более 180 дней (обяз.)
Группа "Журнал"			
Максимальный размер журнала защиты	1Б,1В: Не менее 4096 (реком.) 1Г,1Д: Не менее 2048 (реком.)	2А: Не менее 4096 (реком.) 2Б: Не менее 2048 (реком.)	все: Не менее 2048 (реком.)
Политика перезаписи событий	все: Затирать события по мере необходимости (реком.)	все: Затирать события по мере необходимости (реком.)	все: Затирать события по мере необходимости (реком.)
Учетные записи с привилегией просмотра журнала системы защиты	все: Локальная группа администраторов (реком.)	все: Локальная группа администраторов (реком.)	все: Локальная группа администраторов (реком.)
Учетные записи с привилегией управления журналом системы защиты	все: Локальная группа администраторов (реком.)	все: Локальная группа администраторов (реком.)	все: Локальная группа администраторов (реком.)
Группа "Ключи пользователя"			
Максимальный срок действия ключа	все: Не более 360 (реком.)	все: Не более 360 (реком.)	все: Не более 360 (реком.)
Минимальный срок действия ключа	все: 30 (реком.)	все: 30 (реком.)	все: 30 (реком.)

Параметр	Классы защищенности АС		
	1Б, 1В, 1Г, 1Д	**2А, 2Б**	**3А, 3Б**
Предупреждение об истечении срока действия ключа	все: Не менее 14 (реком.)	все: Не менее 14 (реком.)	все: Не менее 14 (реком.)
Группа "Оповещение о тревогах"			
Локальное оповещение о тревогах	1Б: Включено (обяз.) 1В,1Г,1Д: Включено (реком.)	все: Включено (реком.)	все: Включено (реком.)
Группа "Контроль RDP-подключений"			
Перенаправление устройств в RDP-подключениях	1Б, 1В,1Г: COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.) 1Д:-	2А: COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.) 2Б:-	3А: COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.) 3Б:-
Перенаправление буфера обмена в RDP-подключениях	1Б, 1В: Запрещено (реком.) 1Г,1Д: -	2А: Запрещено (реком.) 2Б: -	3А: Запрещено (реком.) 3Б: -
Перенаправление принтеров в RDP-подключениях	1Б, 1В,1Г: Запрещено (реком.) 1Д:-	2А: Запрещено (реком.) 2Б:-	3А: Запрещено (реком.) 3Б:-
Группа "Контроль административных привилегий"			
Самозащита продукта	все: Включить (обяз.)	все: Включить (обяз.)	все: Включить (обяз.)
Учетные записи с привилегией управления механизмом самозащиты	все: Локальная группа администраторов (реком.)	все: Локальная группа администраторов (реком.)	все: Локальная группа администраторов (реком.)
Группа "Дискреционное управление доступом"			
Учетные записи с привилегией управления правами доступа	1Б,1В,1Г: Локальная группа администраторов (обяз.) 1Д: Локальная группа администраторов (реком.)	все: –	все: –
Группа "Затирание данных"			
Количество циклов затирания на локальных дисках	1Б,1В: Не менее 2 (обяз.) 1Г: Не менее 1 (обяз.) 1Д: –	2А: Не менее 2 (обяз.) 2Б: –	3А: Не менее 2 (обяз.) 3Б: –

Параметр	Классы защищенности АС		
	1Б, 1В, 1Г, 1Д	**2А, 2Б**	**3А, 3Б**
Количество циклов затирания на сменных носителях	1Б,1В: Не менее 2 (обяз.) 1Г: Не менее 1 (обяз.) 1Д: –	2А: Не менее 2 (обяз.) 2Б: –	3А: Не менее 2 (обяз.) 3Б: –
Количество циклов затирания оперативной памяти	1Б,1В: Не менее 2 (обяз.) 1Г: Не менее 1 (обяз.) 1Д: –	2А: Не менее 2 (обяз.) 2Б: –	3А: Не менее 2 (обяз.) 3Б: –
Количество циклов затирания по команде "Удалить безвозвратно"	1Б,1В: Не менее 2 (обяз.) 1Г: Не менее 1 (обяз.) 1Д: –	2А: Не менее 2 (обяз.) 2Б: –	3А: Не менее 2 (обяз.) 3Б: –
Количество циклов затирания при уничтожении данных на дисках	1Б,1В: Не менее 2 (обяз.) 1Г: Не менее 1 (обяз.) 1Д: –	2А: Не менее 2 (обяз.) 2Б: –	3А: Не менее 2 (обяз.) 3Б: –
Группа "Полномочное управление доступом"			
Названия уровней конфиденциальности	1Б,1В: Настроено (обяз.) 1Г,1Д: –	2А: Настроено (обяз.) 2Б: –	все: –
Режим скрытия	1Б,1В: Скрывать недоступные конфиденциальные файлы (реком.) 1Г,1Д: –	все: –	все: –
Режим работы	1Б,1В: Контроль потоков включен (обяз.) 1Г,1Д: –	2А: Контроль потоков включен (обяз.) 2Б: –	все: –
Режим работы: Строгий контроль терминальных подключений	1Б,1В: Да (реком.) 1Г,1Д: –	2А: Да (реком.) 2Б: –	все: –
Группа "Замкнутая программная среда"			
Учетные записи, на которые не действуют правила замкнутой программной среды	1Б,1В: Локальная группа администраторов (реком.) 1Г,1Д: –	2А: Локальная группа администраторов (реком.) 2Б: –	все: –
Группа "Межсетевой экран"			
Правила доступа	все: Настроено (реком.)	все: Настроено (реком.)	все: Настроено (реком.)
Протоколы	все: Включен доступ только для протокола IPv4 (обяз.)	все: Включен доступ только для протокола IPv4 (обяз.)	все: Включен доступ только для протокола IPv4 (обяз.)
Включить ICMP-защиту	1Б,1В: Да (реком.) 1Г,1Д: –	2А: Да (реком.) 2Б: –	3А: Да (реком.) 3Б: –
ICMP-сообщения: Эхо-ответ	1Б,1В: Получение (реком.) 1Г,1Д: –	2А: Получение (реком.) 2Б: –	3А: Получение (реком.) 3Б: –

Параметр	Классы защищенности АС		
	1Б, 1В, 1Г, 1Д	**2А, 2Б**	**3А, 3Б**
ICMP-сообщения: Адресат недоступен	1Б,1В: Получение, Отправка (реком.) 1Г,1Д: –	2А: Получение, Отправка (реком.) 2Б: –	3А: Получение, Отправка (реком.) 3Б: –
ICMP-сообщения: Эхо-запрос	1Б,1В: Отправка (реком.) 1Г,1Д: –	2А: Отправка (реком.) 2Б: –	3А: Отправка (реком.) 3Б: –
ICMP-сообщения: Ходатайство маршрутизатора	1Б,1В: Получение, Отправка (реком.) 1Г,1Д: –	2А: Получение, Отправка (реком.) 2Б: –	3А: Получение, Отправка (реком.) 3Б: –
ICMP-сообщения: Превышение временного интервала	1Б,1В: Получение (реком.) 1Г,1Д: –	2А: Получение (реком.) 2Б: –	3А: Получение (реком.) 3Б: –
ICMP-сообщения: Заблокировать остальные типы	1Б,1В: Да (реком.) 1Г,1Д: –	2А: Да (реком.) 2Б: –	3А: Да (реком.) 3Б: –
Отслеживать состояние соединений	1Б, 1В, 1Г: Вкл (реком.) 1Д: Выкл (реком.)	2А: Вкл (реком.) 2Б: Выкл (реком.)	3А: Вкл (реком.) 3Б: Выкл (реком.)
Блокировать сетевые пакеты, не соответствующие таблице состояний	1Б, 1В, 1Г: Вкл (реком.) 1Д: Выкл (реком.)	2А: Вкл (реком.) 2Б: Выкл (реком.)	3А: Вкл (реком.) 3Б: Выкл (реком.)
Режим обучения	все: Выключен (реком.)	все: Выключен (реком.)	все: Выключен (реком.)
Группа "Авторизация сетевых соединений"			
Защита соединений для группы everyone	1Б,1В,1Г: Да (реком.) 1Д: –	2А: Да (реком.) 2Б: –	все: –
Обработка сетевых пакетов: Параметры обработки сетевых пакетов	1Б,1В,1Г: Подпись, Пакет целиком (обяз.) 1Д: –	2А: Подпись, Пакет целиком (обяз.) 2Б: –	все: –
Обработка сетевых пакетов: Защита от replay-атак	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Группа "Контроль устройств"			
Список устройств: Параметры контроля	1Б,1В,1Г: Параметры заданы, при этом для групп "Устройства USB", "Устройства PCMCIA" и "Устройства IEEE1394" включен режим "Подключение устройства запрещено" (обяз.) 1Д: –	2А: Параметры заданы, при этом для групп "Устройства USB", "Устройства PCMCIA" и "Устройства IEEE1394" включен режим "Подключение устройства запрещено" (обяз.) 2Б: –	все: –
Список устройств: Разрешения	1Б,1В,1Г: Заданы (обяз.) 1Д: –	2А: Заданы (обяз.) 2Б: –	все: –
Группа "Контроль печати"			

Параметр	Классы защищенности АС		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Маркировка документов	1Б,1В: Стандартная обработка (обяз.) 1Г,1Д: –	2А: Стандартная обработка (обяз.) 2Б: –	3А: Стандартная обработка (обяз.) 3Б: –
Список принтеров: Разрешения	1Б,1В,1Г: Заданы (обяз.) 1Д: –	2А: Заданы (обяз.) 2Б: –	все: –

Параметры пользователей

Для соответствия классам защищенности АС должны быть настроены параметры пользователей, перечисленные в следующей таблице. Настройка параметров осуществляется в Центре управления пользователями в диалоговом окне настройки свойств пользователя.

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.10 Параметры пользователей

Параметр	Классы защищенности АС		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Группа параметров "Доступ" в диалоге "Параметры безопасности"			
Уровень допуска	1Б,1В: Назначен уполномоченным пользователям (обяз.) 1Г,1Д: –	2А: Назначен уполномоченным пользователям (обяз.) 2Б: –	все: –
Привилегия: Печать конфиденциальных документов	1Б,1В: Назначена уполномоченным пользователям (обяз.) 1Г,1Д: –	2А: Назначена уполномоченным пользователям (обяз.) 2Б: –	все: –
Привилегия: Управление категориями конфиденциальности	1Б,1В: Назначена уполномоченным пользователям (обяз.) 1Г,1Д: –	2А: Назначена уполномоченным пользователям (обяз.) 2Б: –	все: –
Привилегия: Вывод конфиденциальной информации	1Б,1В: Назначена уполномоченным пользователям (обяз.) 1Г,1Д: –	2А: Назначена уполномоченным пользователям (обяз.) 2Б: –	все: –

Параметры механизмов КЦ и ЗПС

Для соответствия классам защищенности АС должны быть настроены параметры механизмов КЦ и ЗПС, перечисленные в следующей таблице. Настройка параметров осуществляется в программе "Контроль программ и данных".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;

- "–" — значение параметра на усмотрение администратора безопасности.

Табл.11 Параметры механизмов КЦ и ЗПС

Параметр	Классы защищенности АС		
	1Б, 1В, 1Г, 1Д	**2А, 2Б**	**3А, 3Б**
Диалог "Режимы" в диалоговом окне настройки свойств компьютера			
Режим ЗПС включен	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Мягкий режим	1Б,1В: Нет (реком.) 1Г,1Д: –	2А: Нет (реком.) 2Б: – —	все:—
Проверять целостность модулей перед запуском	1Б,1В: Да (обяз.) 1Г,1Д: –	2А: Да (обяз.) 2Б: –	все: –
Проверять заголовки модулей перед запуском	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Контролировать исполняемые скрипты	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Диалоговое окно настройки параметров задания контроля СЗИ			
Метод контроля ресурсов	все: Содержимое (обяз.)	все: –	все: –
Алгоритм	1Б: Имитовставка (реком.) 1В,1Г,1Д: CRC32 (реком.)	все:—	все: –
Регистрация событий: Успех завершения	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Регистрация событий: Ошибка завершения	все: Да (обяз.)	все: Да (обяз.)	все: Да (обяз.)
Регистрация событий: Ошибка проверки	все: Да (обяз.)	все: Да (обяз.)	все: Да (обяз.)
Реакция на отказ: Действия	все: Заблокировать компьютер (реком.)	все: Заблокировать компьютер (реком.)	все: Заблокировать компьютер (реком.)
Расписание	1Б: При загрузке ОС и по расписанию(обяз.) 1В,1Г,1Д: При загрузке ОС или чаще (обяз.)	все: При загрузке ОС или чаще (обяз.)	все: При загрузке ОС или чаще (обяз.)
Диалоговое окно настройки параметров заданий контроля ОС (файлы и реестр)			
Метод контроля ресурсов	все: Содержимое (реком.)	все: –	все: –
Алгоритм	1Б: Имитовставка (реком.) 1В,1Г,1Д: CRC32 для реестра и встроенная ЭЦП для файлов (реком.)	все: –	все: –
Регистрация событий: Успех завершения	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Регистрация событий: Ошибка завершения	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Регистрация событий: Успех проверки	все: Нет (реком.)	все: Нет (реком.)	все: Нет (реком.)
Регистрация событий: Ошибка проверки	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)

Параметр	Классы защищенности АС		
	1Б, 1В, 1Г, 1Д	2А, 2Б	3А, 3Б
Реакция на отказ: Действия	все: Заблокировать компьютер (реком.)	все: Заблокировать компьютер (реком.)	все: Заблокировать компьютер (реком.)
Расписание	1Б: При загрузке ОС и по расписанию (реком.) 1В,1Г,1Д: При загрузке ОС или чаще (реком.)	все: При загрузке ОС или чаще (реком.)	все: При загрузке ОС или чаще (реком.)

Государственные информационные системы

При определенных вариантах настройки система Secret Net Studio обеспечивает соответствие требованиям для государственных информационных систем, изложенным в следующих нормативно-методических документах:

- "Меры защиты информации в государственных информационных системах" (документ утвержден ФСТЭК России 11 февраля 2014 г.).
- "Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17).

Для классов защищенности ГИС К1, К2, К3 и К4 определены базовые наборы мер защиты информации. Организационные и технические меры защиты информации должны обеспечивать реализацию следующих основных требований:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных.

Использование средств доверенной загрузки

В ГИС классов К1 и К2 должны применяться средства доверенной загрузки операционной системы. В качестве средства доверенной загрузки может использоваться изделие "Программно-аппаратный комплекс "Соболь".

Обеспечение непрерывности функционирования

Для обеспечения непрерывности функционирования Secret Net Studio в ГИС всех классов защищенности рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net Studio

Для соответствия классам защищенности ГИС должны быть настроены параметры политик, перечисленные в следующей таблице. Настройка выполняется в Центре управления на вкладке "Настройки", раздел "Политики".

Условные обозначения:

- "Да" — включить параметр;

- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.12 Параметры политик

Параметр	Классы защищенности ГИС		
	К1	К2	К3
Группа "Вход в систему"			
Максимальный период неактивности до блокировки экрана	Не более 5 (обяз.)	Не более 15 (реком.)	Не более 15 (реком.)
Запрет вторичного входа в систему	Да (реком.)	Да (реком.)	Да (реком.)
Количество неудачных попыток аутентификации	От 3 до 4 (обяз.)	От 3 до 8 (обяз.)	От 3 до 10 (обяз.)
Время блокировки при достижении количества неудачных попыток аутентификации	От 15 до 60 (обяз.)	От 10 до 30 (обяз.)	От 3 до 30 (обяз.)
Режим идентификации пользователя	Только по идентификатору (обяз.)	Только по идентификатору (реком.)	Смешанный (реком.)
Режим аутентификации пользователя	Усиленная аутентификация по паролю (обяз.)	Усиленная аутентификация по паролю (обяз.)	Усиленная аутентификация по паролю (обяз.)
Парольная политика	Задать свои значения (обяз.)	Задать свои значения (обяз.)	Задать свои значения (обяз.)
Минимальная длина пароля	Не менее 8 символов (обяз.)	Не менее 6 символов (обяз.)	Не менее 6 символов (обяз.)
Срок действия пароля	Не более 60 дней (обяз.)	Не более 90 дней (обяз.)	Не более 120 дней (обяз.)
Сложность пароля	Да (обяз.)	Да (обяз.)	Да (обяз.)
Группа "Журнал"			
Максимальный размер журнала защиты	Не менее 4096 (реком.)	Не менее 4096 (реком.)	Не менее 4096 (реком.)
Политика перезаписи событий	Затирать события по мере необходимости (реком.)	Затирать события по мере необходимости (реком.)	Затирать события по мере необходимости (реком.)
Учетные записи с привилегией просмотра журнала системы защиты	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Учетные записи с привилегией управления журналом системы защиты	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Ключи пользователя"			
Максимальный срок действия ключа	Не более 360 (реком.)	Не более 360 (реком.)	Не более 360 (реком.)

Параметр	Классы защищенности ГИС		
	К1	К2	К3
Минимальный срок действия ключа	30 (реком.)	30 (реком.)	30 (реком.)
Предупреждение об истечении срока действия ключа	Не менее 14 (реком.)	Не менее 14 (реком.)	Не менее 14 (реком.)
Группа "Оповещение о тревогах"			
Локальное оповещение о тревогах	Включено (реком.)	Включено (реком.)	Включено (реком.)
Группа "Контроль RDP-подключений"			
Перенаправление устройств в RDP-подключениях	COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.)	COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.)	COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.)
Группа "Контроль административных привилегий"			
Самозащита продукта	Включить (обяз.)	Включить (обяз.)	Включить (обяз.)
Учетные записи с привилегией управления механизмом самозащиты	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Дискреционное управление доступом"			
Учетные записи с привилегией управления правами доступа	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Затирание данных"			
Количество циклов затирания на локальных дисках	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)
Количество циклов затирания на сменных носителях	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)
Количество циклов затирания оперативной памяти	Не менее 2 (обяз.)	–	–
Количество циклов затирания по команде "Удалить безвозвратно"	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)
Количество циклов затирания при уничтожении данных на дисках	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)
Группа "Полномочное управление доступом"			
Названия уровней конфиденциальности	Настроено (обяз.)*	–	–

Параметр	Классы защищенности ГИС		
	К1	К2	К3
Режим работы	Контроль потоков включен (обяз.)*	–	–
Режим работы: Строгий контроль терминальных подключений	Да (обяз.)*	–	–
Группа "Замкнутая программная среда"			
Учетные записи, на которые не действуют правила замкнутой программной среды	Локальная группа администраторов (реком.)	–	–
Группа "Межсетевой экран"			
Правила доступа	Настроено (реком.)	Настроено (реком.)	Настроено (реком.)
Протоколы	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)
Включить ICMP-защиту	Да (реком.)	Да (реком.)	–
ICMP-сообщения: Эхо-ответ	Получение (реком.)	Получение (реком.)	–
ICMP-сообщения: Адресат недоступен	Получение, Отправка (реком.)	Получение, Отправка (реком.)	–
ICMP-сообщения: Эхо-запрос	Отправка (реком.)	Отправка (реком.)	–
ICMP-сообщения: Ходатайство маршрутизатора	Получение, Отправка (реком.)	Получение, Отправка (реком.)	–
ICMP-сообщения: Превышение временного интервала	Получение (реком.)	Получение (реком.)	–
ICMP-сообщения: Заблокировать остальные типы	Да (реком.)	Да (реком.)	–
Отслеживать состояние соединений	Вкл (обяз.)	Выкл (реком.)	Выкл (реком.)
Блокировать сетевые пакеты, не соответствующие таблице состояний	Вкл (обяз.)	Выкл (реком.)	Выкл (реком.)
Режим обучения	Выключен (реком.)	Выключен (реком.)	Выключен (реком.)
Группа "Авторизация сетевых соединений"			
Защита соединений для группы everyone	Да (реком.)	Да (реком.)	–
Обработка сетевых пакетов: Параметры обработки сетевых пакетов	Подпись, Пакет целиком (обяз.)	Подпись, Пакет целиком (обяз.)	–
Обработка сетевых пакетов: Защита от replay-атак	Да (реком.)	Да (реком.)	Да (реком.)

Параметр	Классы защищенности ГИС		
	К1	К2	К3
Группа "Контроль устройств"			
Список устройств: Параметры контроля	Параметры заданы, при этом для групп "Устройства USB", "Устройства PCMCIA" и "Устройства IEEE1394" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для групп "Устройства USB", "Устройства PCMCIA" и "Устройства IEEE1394" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для групп "Устройства USB", "Устройства PCMCIA" и "Устройства IEEE1394" включен режим "Подключение устройства запрещено" (обяз.)
Список устройств: Разрешения	Заданы (обяз.)	Заданы (обяз.)	Заданы (обяз.)
Группа "Контроль печати"			
Список принтеров: Разрешения	Заданы (обяз.)	Заданы (обяз.)	Заданы (обяз.)

*Действие является обязательным, если для реализации меры ОЦЛ.6 (ограничение прав пользователей по вводу информации в систему) будет применяться механизм полномочного управления доступом системы Secret Net Studio. Если для реализации указанной меры защиты применяются другие решения, действие не обязательно для выполнения.

Параметры пользователей

Для соответствия классам защищенности ГИС должны быть настроены параметры пользователей, перечисленные в следующей таблице. Настройка параметров осуществляется в Центре управления пользователями в диалоговом окне настройки свойств пользователя.

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.13 Параметры пользователей

Параметр	Классы защищенности ГИС		
	К1	К2	К3
Группа параметров "Идентификатор" в диалоге "Параметры безопасности"			
Электронный идентификатор пользователя	Присвоен (обяз.)	Присвоен (реком.)	–
Интеграция с ПАК "Соболь"	Да (реком.)	Да (реком.)	–
Группа параметров "Доступ" в диалоге "Параметры безопасности"			
Уровень допуска	Назначен уполномоченным пользователям (обяз.)*	–	–

Параметр	Классы защищенности ГИС		
	К1	К2	К3
Привилегия: Управление категориями конфиденциальности	Назначена уполномоченным пользователям (обяз.)*	–	–

*Действие является обязательным, если для реализации меры ОЦЛ.6 (ограничение прав пользователей по вводу информации в систему) будет применяться механизм полномочного управления доступом системы Secret Net Studio. Если для реализации указанной меры защиты применяются другие решения, действие не обязательно для выполнения.

Параметры механизмов КЦ и ЗПС

Для соответствия классам защищенности ГИС должны быть настроены параметры механизмов КЦ и ЗПС, перечисленные в следующей таблице. Настройка параметров осуществляется в программе "Контроль программ и данных".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.14 Параметры механизмов КЦ и ЗПС

Параметр	Классы защищенности ГИС		
	К1	К2	К3
Диалог "Режимы" в диалоговом окне настройки свойств компьютера			
Режим ЗПС включен	Да (обяз.)	–	–
Мягкий режим	Нет (обяз.)	–	–
Проверять целостность модулей перед запуском	Да (обяз.)	–	–
Проверять заголовки модулей перед запуском	Да (реком.)	–	–
Контролировать исполняемые скрипты	Да (реком.)	–	–
Диалоговое окно настройки параметров задания контроля СЗИ			
Метод контроля ресурсов	Содержимое (обяз.)	Содержимое (обяз.)	–
Алгоритм	CRC32 (реком.)	CRC32 (реком.)	–
Регистрация событий: Успех завершения	Да (реком.)	Да (реком.)	–
Регистрация событий: Ошибка завершения	Да (обяз.)	Да (обяз.)	–
Регистрация событий: Ошибка проверки	Да (обяз.)	Да (обяз.)	–
Реакция на отказ: Действия	Заблокировать компьютер (реком.)	Заблокировать компьютер (реком.)	–
Расписание	При загрузке ОС и по расписанию (обяз.)	При загрузке ОС и по расписанию (обяз.)	–
Диалоговое окно настройки параметров задания контроля ОС (файлы и реестр)			
Метод контроля ресурсов	Содержимое (реком.)	Содержимое (реком.)	–

Параметр	Классы защищенности ГИС		
	К1	К2	К3
Алгоритм	CRC32 (реком.)	CRC32 (реком.)	–
Регистрация событий: Успех завершения	Да (реком.)	Да (реком.)	–
Регистрация событий: Ошибка завершения	Да (реком.)	Да (реком.)	–
Регистрация событий: Успех проверки	Нет (реком.)	Нет (реком.)	–
Регистрация событий: Ошибка проверки	Да (реком.)	Да (реком.)	–
Реакция на отказ: Действия	Заблокировать компьютер (реком.)	Заблокировать компьютер (реком.)	–
Расписание	При загрузке ОС и по расписанию (реком.)	При загрузке ОС и по расписанию (реком.)	–

Информационные системы персональных данных

При определенных вариантах настройки система Secret Net Studio обеспечивает соответствие требованиям для информационных систем персональных данных (ИСПДн), изложенным в документе "Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (утвержден приказом ФСТЭК России от 18 февраля 2013 г. № 21).

Для уровней защищенности ИСПДн 1, 2, 3 и 4 определены базовые наборы мер защиты информации. Организационные и технические меры защиты информации должны обеспечивать реализацию следующих основных требований:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее — машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее — инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

Использование средств доверенной загрузки

В ИСПДн уровней 1 и 2 должны применяться средства доверенной загрузки операционной системы. В качестве средства доверенной загрузки может использоваться изделие "Программно-аппаратный комплекс "Соболь".

Обеспечение непрерывности функционирования

Для обеспечения непрерывности функционирования Secret Net Studio в ИСПДн всех уровней защищенности рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net Studio

Для соответствия уровням защищенности ИСПДн должны быть настроены параметры политик, перечисленные в следующей таблице. Настройка параметров осуществляется в Центре управления на вкладке "Настройки", раздел "Политики".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.15 Параметры политик

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Группа "Вход в систему"				
Максимальный период неактивности до блокировки экрана	Не более 5 (обяз.)	Не более 15 (реком.)	Не более 15 (реком.)	Не более 15 (реком.)
Запрет вторичного входа в систему	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Количество неудачных попыток аутентификации	От 3 до 4 (обяз.)	От 3 до 8 (обяз.)	От 3 до 10 (обяз.)	От 3 до 10 (обяз.)
Время блокировки при достижении количества неудачных попыток аутентификации	От 15 до 60 (обяз.)	От 10 до 30 (обяз.)	От 5 до 30 (обяз.)	От 3 до 15 (обяз)
Режим идентификации пользователя	Только по идентификатору (обяз.)	Только по идентификатору (реком.)	Смешанный (реком.)	Смешанный (реком.)
Режим аутентификации пользователя	Усиленная аутентификация по паролю (обяз.)	Усиленная аутентификация по паролю (обяз.)	Усиленная аутентификация по паролю (обяз.)	Усиленная аутентификация по паролю (обяз.)
Парольная политика	Задать свои значения (обяз.)	Задать свои значения (обяз.)	Задать свои значения (обяз.)	Задать свои значения (обяз.)
Минимальная длина пароля	Не менее 8 символов (обяз.)	Не менее 6 символов (обяз.)	Не менее 6 символов (обяз.)	Не менее 6 символов (обяз.)
Срок действия пароля	Не более 60 дней (обяз.)	Не более 90 дней (обяз.)	Не более 120 дней (обяз.)	Не более 180 дней (обяз.)
Сложность пароля	Да (обяз.)	Да (обяз.)	Да (обяз.)	Да (обяз.)
Группа "Журнал"				

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Максимальный размер журнала защиты	Не менее 4096 (реком.)	Не менее 4096 (реком.)	Не менее 4096 (реком.)	Не менее 4096 (реком.)
Политика перезаписи событий	Затирать события по мере необходимости (реком.)	Затирать события по мере необходимости (реком.)	Затирать события по мере необходимости (реком.)	Затирать события по мере необходимости (реком.)
Учетные записи с привилегией просмотра журнала системы защиты	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Учетные записи с привилегией управления журналом системы защиты	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Ключи пользователя"				
Максимальный срок действия ключа	Не более 360 (реком.)	Не более 360 (реком.)	Не более 360 (реком.)	Не более 360 (реком.)
Минимальный срок действия ключа	30 (реком.)	30 (реком.)	30 (реком.)	30 (реком.)
Предупреждение об истечении срока действия ключа	Не менее 14 (реком.)	Не менее 14 (реком.)	Не менее 14 (реком.)	Не менее 14 (реком.)
Группа "Оповещение о тревогах"				
Локальное оповещение о тревогах	Включено (реком.)	Включено (реком.)	Включено (реком.)	Включено (реком.)
Группа "Контроль RDP-подключений"				
Перенаправление устройств в RDP-подключениях	COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.)	COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.)	-	-
Группа "Контроль административных привилегий"				
Самозащита продукта	Включить (обяз.)	Включить (обяз.)	Включить (обяз.)	Включить (обяз.)
Учетные записи с привилегией управления механизмом самозащиты	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Дискреционное управление доступом"				
Учетные записи с привилегией управления правами доступа	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Затирание данных"				
Количество циклов затирания на локальных дисках	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)	–

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Количество циклов затирания на сменных носителях	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)	–
Количество циклов затирания по команде "Удалить безвозвратно"	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)	–
Количество циклов затирания при уничтожении данных на дисках	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)	–
Группа "Полномочное управление доступом"				
Названия уровней конфиден-циальности	Настроено (обяз.)*	–	–	–
Режим работы	Контроль потоков включен (обяз.)*	–	–	–
Режим работы: Строгий контроль терминальных подключений	Да (обяз.)*	–	–	–
Группа "Межсетевой экран"				
Правила доступа	Настроено (реком.)	Настроено (реком.)	Настроено (реком.)	Настроено (реком.)
Протоколы	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)
Включить ICMP-защиту	Да (реком.)	Да (реком.)	–	–
ICMP-сообщения: Эхо-ответ	Получение (реком.)	Получение (реком.)	–	–
ICMP-сообщения: Адресат недоступен	Получение, Отправка (реком.)	Получение, Отправка (реком.)	–	–
ICMP-сообщения: Эхо-запрос	Отправка (реком.)	Отправка (реком.)	–	–
ICMP-сообщения: Ходатайство маршрутиза-тора	Получение, Отправка (реком.)	Получение, Отправка (реком.)	–	–
ICMP-сообщения: Превышение временного интервала	Получение (реком.)	Получение (реком.)	–	–
ICMP-сообщения: Заблокировать остальные типы	Да (реком.)	Да (реком.)	–	–
Отслеживать состояние соединений	Вкл (обяз.)	Выкл (реком.)	Выкл (реком.)	Выкл (реком.)
Блокировать сетевые пакеты, не соответствующие таблице состояний	Вкл (обяз.)	Выкл (реком.)	Выкл (реком.)	Выкл (реком.)
Режим обучения	Выключен (реком.)	Выключен (реком.)	Выключен (реком.)	Выключен (реком.)
Группа "Авторизация сетевых соединений"				
Защита соединений для группы everyone	Да (реком.)	Да (реком.)	–	–

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Обработка сетевых пакетов: Параметры обработки сетевых пакетов	Подпись, Пакет целиком (обяз.)	Подпись, Пакет целиком (обяз.)	–	–
Обработка сетевых пакетов: Защита от replay-атак	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Группа "Контроль устройств"				
Список устройств: Параметры контроля	Параметры заданы, при этом для групп "Устройства USB", "Устройства PCMCIA" и "Устройства IEEE1394" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для групп "Устройства USB", "Устройства PCMCIA" и "Устройства IEEE1394" включен режим "Подключение устройства запрещено" (обяз.)	–	–
Список устройств: Разрешения	Заданы (обяз.)	Заданы (обяз.)	–	–
Группа "Контроль печати"				
Список принтеров: Разрешения	Заданы (обяз.)	Заданы (обяз.)	–	–

*Действие является обязательным, если для реализации меры ОЦЛ.6 (ограничение прав пользователей по вводу информации в систему) будет применяться механизм полномочного управления доступом системы Secret Net Studio. Если для реализации указанной меры защиты применяются другие решения, действие не обязательно для выполнения.

Параметры пользователей

Для соответствия уровням защищенности ИСПДн должны быть настроены параметры пользователей, перечисленные в следующей таблице. Настройка параметров осуществляется в Центре управления пользователями в диалоговом окне настройки свойств пользователя.

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.16 Параметры пользователей

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Группа параметров "Идентификатор" в диалоге "Параметры безопасности"				
Электронный идентификатор пользователя	Присвоен (обяз.)	Присвоен (реком.)	–	–
Интеграция с ПАК "Соболь"	Да (реком.)	Да (реком.)	–	–
Группа параметров "Доступ" в диалоге "Параметры безопасности"				

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Уровень допуска	Назначен уполномоченным пользователям (обяз.)*	–	–	–
Привилегия: Управление категориями конфиденциальности	Назначена уполномоченным пользователям (обяз.)*	–	–	–

*Действие является обязательным, если для реализации меры ОЦЛ.6 (ограничение прав пользователей по вводу информации в систему) будет применяться механизм полномочного управления доступом системы Secret Net Studio. Если для реализации указанной меры защиты применяются другие решения, действие не обязательно для выполнения.

Параметры механизмов КЦ и ЗПС

Для соответствия уровням защищенности ИСПДн должны быть настроены параметры механизмов КЦ и ЗПС, перечисленные в следующей таблице. Настройка параметров осуществляется в программе "Контроль программ и данных".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.17 Параметры механизмов КЦ и ЗПС

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Диалоговое окно настройки параметров задания контроля СЗИ				
Метод контроля ресурсов	Содержимое (обяз.)	Содержимое (обяз.)	–	–
Алгоритм	CRC32 (реком.)	CRC32 (реком.)	–	–
Регистрация событий: Успех завершения	Да (реком.)	Да (реком.)	–	–
Регистрация событий: Ошибка завершения	Да (обяз.)	Да (обяз.)	–	–
Регистрация событий: Ошибка проверки	Да (обяз.)	Да (обяз.)	–	–
Реакция на отказ: Действия	Заблокировать компьютер (реком.)	Заблокировать компьютер (реком.)	–	–
Расписание	При загрузке ОС и по расписанию (обяз.)	При загрузке ОС и по расписанию (обяз.)	–	–
Диалоговое окно настройки параметров задания контроля ОС (файлы и реестр)				
Метод контроля ресурсов	Содержимое (реком.)	Содержимое (реком.)	–	–
Алгоритм	CRC32 (реком.)	CRC32 (реком.)	–	–

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Регистрация событий: Успех завершения	Да (реком.)	Да (реком.)	–	–
Регистрация событий: Ошибка завершения	Да (реком.)	Да (реком.)	–	–
Регистрация событий: Успех проверки	Нет (реком.)	Нет (реком.)	–	–
Регистрация событий: Ошибка проверки	Да (реком.)	Да (реком.)	–	–
Реакция на отказ: Действия	Заблокировать компьютер (реком.)	Заблокировать компьютер (реком.)	–	–
Расписание	При загрузке ОС и по расписанию (реком.)	При загрузке ОС и по расписанию (реком.)	–	–

Информационные системы Банка России

При определенных вариантах настройки система Secret Net Studio обеспечивает соответствие требованиям, установленным Банком России к объектам информатизации (в том числе АС) финансовых организаций, изложенным в следующем стандарте:

- ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер (утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. № 822-ст).

Для уровней защиты информации ИС Банка России УЗ-1, УЗ-2 и УЗ-3 определены базовые наборы мер защиты информации. Организационные и технические меры защиты информации должны обеспечивать реализацию следующих основных требований для следующих процессов (направлений) защиты информации:

- процесс 1 "Обеспечение защиты информации при управлении доступом":
  - управление учетными записями и правами субъектов логического доступа:
    - идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа;
    - защита информации при осуществлении физического доступа;
    - идентификация, классификация и учет ресурсов и объектов доступа;
- процесс 2 "Обеспечение защиты вычислительных сетей":
  - сегментация и межсетевое экранирование вычислительных сетей;
  - выявление сетевых вторжений и атак:
    - защита информации, передаваемой по вычислительным сетям;
    - защита беспроводных сетей;
- процесс 3 "Контроль целостности и защищенности информационной инфраструктуры";
- процесс 4 "Защита от вредоносного кода";
- процесс 5 "Предотвращение утечек информации";
- процесс 6 "Управление инцидентами защиты информации":
  - мониторинг и анализ событий защиты информации;
  - обнаружение инцидентов защиты информации и реагирование на них;
- процесс 7 "Защита среды виртуализации";

- процесс 8 "Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств".

Использование средств доверенной загрузки

В ИС Банка России уровня защиты информации УЗ-1 должны применяться средства доверенной загрузки операционной системы. В качестве средства доверенной загрузки может использоваться изделие "Программно-аппаратный комплекс "Соболь".

Обеспечение непрерывности функционирования

Для обеспечения непрерывности функционирования Secret Net Studio в ИС Банка России всех уровней защиты информации рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net Studio

Для соответствия уровням защиты информации ИС Банка России должны быть настроены параметры политик, перечисленные в следующей таблице. Настройка выполняется в Центре управления на вкладке "Настройки", раздел "Политики".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.18 Параметры политик

Параметр	Уровень защиты информации ИС Банка России		
	УЗ-1	**УЗ-2**	**УЗ-3**
Группа "Вход в систему"			
Максимальный период неактивности до блокировки экрана	Не более 15 (обяз.)	Не более 15 (реком.)	Не более 15 (реком.)
Запрет вторичного входа в систему	Да (реком.)	Да (реком.)	Да (реком.)
Время блокировки при достижении количества неудачных попыток аутентификации	Не менее 30 минут (обяз.)	Не менее 30 минут (обяз.)	Не менее 30 минут (обяз.)
Режим идентификации пользователя	Только по идентификатору (обяз.)	Только по идентификатору (реком.)	все: Смешанный (реком.)
Режим аутентификации пользователя	Усиленная аутентификация по паролю (обяз.)	Усиленная аутентификация по паролю (обяз.)	Усиленная аутентификация по паролю (обяз.)
Парольная политика	Задать свои значения (обяз.)	Задать свои значения (обяз.)	Задать свои значения (обяз.)
Минимальная длина пароля	Не менее 8 символов (обяз.) Пароль Администратора не менее 16 символов	Не менее 6 символов (обяз.) Пароль Администратора не менее 16 символов	Не менее 6 символов (обяз.) Пароль Администратора не менее 16 символов

Параметр	Уровень защиты информации ИС Банка России		
	УЗ-1	**УЗ-2**	**УЗ-3**
Срок действия пароля	Не более 60 дней (обяз.) Для Администратора не более 90 дней	Не более 90 дней (обяз.) Для Администратора не более 90 дней	Не более 120 дней (обяз.) Для Администратора не более 90 дней
Сложность пароля	Да (обяз.)	Да (обяз.)	Да (обяз.)
Оповещение пользователя о последнем успешном входе в систему	Да (обяз.)	-	-
Группа "Журнал"			
Максимальный размер журнала защиты	Не менее 4096 (реком.)	Не менее 4096 (реком.)	Не менее 4096 (реком.)
Политика перезаписи событий	Затирать события по мере необходимости (реком.)	Затирать события по мере необходимости (реком.)	Затирать события по мере необходимости (реком.)
Учетные записи с привилегией просмотра журнала системы защиты	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Учетные записи с привилегией управления журналом системы защиты	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Ключи пользователя"			
Максимальный срок действия ключа	Не более 360 (реком.)	Не более 360 (реком.)	Не более 360 (реком.)
Минимальный срок действия ключа	30 (реком.)	30 (реком.)	30 (реком.)
Предупреждение об истечении срока действия ключа	Не менее 14 (реком.)	Не менее 14 (реком.)	Не менее 14 (реком.)
Группа "Оповещение о тревогах"			
Локальное оповещение о тревогах	Включено (реком.)	Включено (реком.)	Включено (реком.)
Группа "Контроль RDP-подключений"			
Перенаправление устройств в RDP-подключениях	COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.)	COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.)	COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.)
Группа "Контроль административных привилегий"			
Самозащита продукта	все: Включить (обяз.)	все: Включить (обяз.)	все: Включить (обяз.)
Учетные записи с привилегией управления механизмом самозащиты	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)

Параметр	Уровень защиты информации ИС Банка России		
	УЗ-1	УЗ-2	УЗ-3
Группа "Дискреционное управление доступом"			
Учетные записи с привилегией управления правами доступа	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Затирание данных"			
Количество циклов затирания на локальных дисках	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)
Количество циклов затирания на сменных носителях	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)
Количество циклов затирания оперативной памяти	Не менее 2 (обяз.)	-	-
Количество циклов затирания по команде "Удалить безвозвратно"	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)
Количество циклов затирания при уничтожении данных на дисках	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)
Группа "Полномочное управление доступом"			
Названия уровней конфиденциальности	Настроено (обяз.)	–	–
Режим работы	Контроль потоков включен (обяз.)	–	–
Режим работы: Строгий контроль терминальных подключений	Да (обяз.)	–	–
Группа "Межсетевой экран"			
Правила доступа	Настроено (реком.)	Настроено (реком.)	Настроено (реком.)
Протоколы	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)
Включить ICMP-защиту	Да (реком.)	Да (реком.)	Да (реком.)
ICMP-сообщения: Эхо-ответ	Получение (реком.)	Получение (реком.)	Получение (реком.)
ICMP-сообщения: Адресат недоступен	Получение, Отправка (реком.)	Получение, Отправка (реком.)	Получение, Отправка (реком.)
ICMP-сообщения: Эхо-запрос	Отправка (реком.)	Отправка (реком.)	Отправка (реком.)
ICMP-сообщения: Ходатайство маршрутизатора	Получение, Отправка (реком.)	Получение, Отправка (реком.)	Получение, Отправка (реком.)
ICMP-сообщения: Превышение временного интервала	Получение (реком.)	Получение (реком.)	Получение (реком.)
ICMP-сообщения: Заблокировать остальные типы	Да (реком.)	Да (реком.)	Да (реком.)
Отслеживать состояние соединений	Вкл (обяз.)	Выкл (реком.)	Выкл (реком.)
Блокировать сетевые пакеты, не соответствующие таблице состояний	Вкл (обяз.)	Выкл (реком.)	Выкл (реком.)
Режим обучения	Выключен (реком.)	Выключен (реком.)	Выключен (реком.)
Группа "Авторизация сетевых соединений"			
Защита соединений для группы everyone	Да (реком.)	Да (реком.)	–
Обработка сетевых пакетов: Параметры обработки сетевых пакетов	Подпись, Пакет целиком (обяз.)	Подпись, Пакет целиком (обяз.)	–

Параметр	Уровень защиты информации ИС Банка России		
	УЗ-1	УЗ-2	УЗ-3
Обработка сетевых пакетов: Защита от replay-атак	Да (реком.)	Да (реком.)	Да (реком.)
Группа "Контроль устройств"			
Список устройств: Параметры контроля	Параметры заданы, при этом для групп "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для групп "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для групп "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)
Список устройств: Разрешения	Заданы (обяз.)	Заданы (обяз.)	Заданы (обяз.)
Группа "Контроль печати"			
Список принтеров: Разрешения	Заданы (обяз.)	Заданы (обяз.)	Заданы (обяз.)

Параметры пользователей

Для соответствия уровням защиты информации ИС Банка России должны быть настроены параметры пользователей, перечисленные в следующей таблице. Настройка параметров осуществляется в Центре управления пользователями в диалоговом окне настройки свойств пользователя.

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.19 Параметры пользователей

Параметр	Уровень защиты информации ИС Банка России		
	УЗ-1	УЗ-2	УЗ-3
Группа параметров "Идентификатор" в диалоге "Параметры безопасности"			
Электронный идентификатор пользователя	Присвоен (обяз.)	–	–
Интеграция с ПАК "Соболь"	Да (реком.)	–	–
Группа параметров "Доступ" в диалоге "Параметры безопасности"			
Уровень допуска	Назначен уполномоченным пользователям (обяз.)*	–	–
Привилегия: Управление категориями конфиденциальности	Назначена уполномоченным пользователям (обяз.)*	–	–

Параметры механизмов КЦ и ЗПС

Для соответствия уровням защиты информации ИС Банка России должны быть настроены параметры механизмов КЦ и ЗПС, перечисленные в следующей таблице. Настройка параметров осуществляется в программе "Контроль программ и данных".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.20 Параметры механизмов КЦ и ЗПС

Параметр	Уровень защиты информации ИС Банка России		
	УЗ-1	**УЗ-2**	**УЗ-3**
Диалог "Режимы" в диалоговом окне настройки свойств компьютера			
Режим ЗПС включен	Да (обяз.)	Да (обяз.)	–
Мягкий режим	Нет (обяз.)	Нет (обяз.)	–
Проверять целостность модулей перед запуском	Да (обяз.)	Да (обяз.)	–
Проверять заголовки модулей перед запуском	Да (реком.)	Да (реком.)	–
Контролировать исполняемые скрипты	Да (реком.)	Да (реком.)	–
Диалоговое окно настройки параметров задания контроля СЗИ			
Метод контроля ресурсов	Содержимое (обяз.)	Содержимое (обяз.)	–
Алгоритм	CRC32 (реком.)	CRC32 (реком.)	–
Регистрация событий: Успех завершения	Да (реком.)	Да (реком.)	–
Регистрация событий: Ошибка завершения	Да (обяз.)	Да (обяз.)	–
Регистрация событий: Ошибка проверки	Да (обяз.)	Да (обяз.)	–
Реакция на отказ: Действия	Заблокировать компьютер (реком.)	Заблокировать компьютер (реком.)	–
Расписание	При загрузке ОС и по расписанию (реком.)	При загрузке ОС и по расписанию (реком.)	–
Диалоговое окно настройки параметров задания контроля ОС (файлы и реестр)			
Метод контроля ресурсов	Содержимое (реком.)	Содержимое (реком.)	–
Алгоритм	CRC32 (реком.)	CRC32 (реком.)	–
Регистрация событий: Успех завершения	Да (реком.)	Да (реком.)	–
Регистрация событий: Ошибка завершения	Да (реком.)	Да (реком.)	–
Регистрация событий: Успех проверки	Нет (реком.)	Нет (реком.)	–
Регистрация событий: Ошибка проверки	Да (реком.)	Да (реком.)	–
Реакция на отказ: Действия	Заблокировать компьютер (реком.)	Заблокировать компьютер (реком.)	–
Расписание	При загрузке ОС и по расписанию (реком.)	При загрузке ОС и по расписанию (реком.)	–

Автоматизированные системы управления производственными и технологическими процессами

При определенных вариантах настройки система Secret Net Studio обеспечивает соответствие требованиям для автоматизированных систем управления производственными и технологическими процессами (АСУ ТП), изложенным в следующем нормативном документе:

- Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (утверждены приказом ФСТЭК России от 14 марта 2014 г. № 31).

Для классов защищенности АСУ ТП К1, К2 и К3 определены базовые наборы мер защиты информации. Организационные и технические меры защиты информации должны обеспечивать реализацию следующих основных требований:

- идентификация и аутентификация;
- управление доступом;
- ограничение программной среды;
- защита машинных носителей информации;
- аудит безопасности;
- антивирусная защита;
- предотвращение вторжений (компьютерных атак);
- обеспечение целостности;
- обеспечение доступности;
- защита технических средств и систем;
- защита информационной (автоматизированной) системы и ее компонентов;
- реагирование на компьютерные инциденты;
- управление конфигурацией;
- управление обновлениями программного обеспечения;
- планирование мероприятий по обеспечению безопасности;
- обеспечение действий в нештатных ситуациях;
- информирование и обучение персонала.

Использование средств доверенной загрузки

В АСУ ТП классов К1 и К2 должны применяться средства доверенной загрузки операционной системы. В качестве средства доверенной загрузки может использоваться изделие "Программно-аппаратный комплекс "Соболь".

Обеспечение непрерывности функционирования

Для обеспечения непрерывности функционирования Secret Net Studio в АСУ ТП всех классов защищенности рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net Studio

Для соответствия классам защищенности АСУ ТП должны быть настроены параметры политик, перечисленные в следующей таблице. Настройка выполняется в Центре управления на вкладке "Настройки", раздел "Политики".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.21 Параметры политик

Параметр	Классы защищенности АСУ ТП		
	К1	К2	К3
Группа "Вход в систему"			
Максимальный период неактивности до блокировки экрана	Не более 5 (обяз.)	Не более 15 (реком.)	Не более 15 (реком.)
Запрет вторичного входа в систему	Да (реком.)	Да (реком.)	Да (реком.)
Количество неудачных попыток аутентификации	От 3 до 4 (обяз.)	От 3 до 8 (обяз.)	От 3 до 10 (обяз.)
Время блокировки при достижении количества неудачных попыток аутентификации	От 15 до 60 (обяз.)	От 10 до 30 (обяз.)	От 3 до 30 (обяз.)
Режим идентификации пользователя	Только по идентификатору (обяз.)	Только по идентификатору (реком.)	Смешанный (реком.)
Режим аутентификации пользователя	Усиленная аутентификация по паролю (обяз.)	Усиленная аутентификация по паролю (обяз.)	Усиленная аутентификация по паролю (обяз.)
Парольная политика	Задать свои значения (обяз.)	Задать свои значения (обяз.)	Задать свои значения (обяз.)
Минимальная длина пароля	Не менее 8 символов (обяз.)	Не менее 6 символов (обяз.)	Не менее 6 символов (обяз.)
Срок действия пароля	Не более 60 дней (обяз.)	Не более 90 дней (обяз.)	Не более 120 дней (обяз.)
Сложность пароля	Да (обяз.)	Да (обяз.)	Да (обяз.)
Группа "Журнал"			
Максимальный размер журнала защиты	Не менее 4096 (реком.)	Не менее 4096 (реком.)	Не менее 4096 (реком.)
Политика перезаписи событий	Затирать события по мере необходимости (реком.)	Затирать события по мере необходимости (реком.)	Затирать события по мере необходимости (реком.)
Учетные записи с привилегией просмотра журнала системы защиты	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Учетные записи с привилегией управления журналом системы защиты	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Ключи пользователя"			
Максимальный срок действия ключа	Не более 360 (реком.)	Не более 360 (реком.)	Не более 360 (реком.)
Минимальный срок действия ключа	30 (реком.)	30 (реком.)	30 (реком.)

Параметр	Классы защищенности АСУ ТП		
	К1	К2	К3
Предупреждение об истечении срока действия ключа	Не менее 14 (реком.)	Не менее 14 (реком.)	Не менее 14 (реком.)
Группа "Оповещение о тревогах"			
Локальное оповещение о тревогах	Включено (реком.)	Включено (реком.)	Включено (реком.)
Группа "Контроль RDP-подключений"			
Перенаправление устройств в RDP-подключениях	COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.)	COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.)	COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.)
Группа "Контроль административных привилегий"			
Самозащита продукта	Включить (обяз.)	Включить (обяз.)	Включить (обяз.)
Учетные записи с привилегией управления механизмом самозащиты	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Дискреционное управление доступом"			
Учетные записи с привилегией управления правами доступа	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Затирание данных"			
Количество циклов затирания на локальных дисках	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)
Количество циклов затирания на сменных носителях	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)
Количество циклов затирания оперативной памяти	Не менее 2 (обяз.)	–	–
Количество циклов затирания по команде "Удалить безвозвратно"	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)
Количество циклов затирания при уничтожении данных на дисках	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)
Группа "Полномочное управление доступом"			
Названия уровней конфиденциальности	Настроено (обяз.)*	–	–
Режим работы	Контроль потоков включен (обяз.)*	–	–
Режим работы: Строгий контроль терминальных подключений	Да (обяз.)*	–	–
Группа "Замкнутая программная среда"			

Параметр	Классы защищенности АСУ ТП		
	К1	К2	К3
Учетные записи, на которые не действуют правила замкнутой программной среды	Локальная группа администраторов (реком.)	–	–
Группа "Межсетевой экран"			
Правила доступа	Настроено (реком.)	Настроено (реком.)	Настроено (реком.)
Протоколы	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)
Включить ICMP-защиту	Да (реком.)	Да (реком.)	–
ICMP-сообщения: Эхо-ответ	Получение (реком.)	Получение (реком.)	–
ICMP-сообщения: Адресат недоступен	Получение, Отправка (реком.)	Получение, Отправка (реком.)	–
ICMP-сообщения: Эхо-запрос	Отправка (реком.)	Отправка (реком.)	–
ICMP-сообщения: Ходатайство маршрутизатора	Получение, Отправка (реком.)	Получение, Отправка (реком.)	–
ICMP-сообщения: Превышение временного интервала	Получение (реком.)	Получение (реком.)	–
ICMP-сообщения: Заблокировать остальные типы	Да (реком.)	Да (реком.)	–
Отслеживать состояние соединений	Вкл (обяз.)	Выкл (реком.)	Выкл (реком.)
Блокировать сетевые пакеты, не соответствующие таблице состояний	Вкл (обяз.)	Выкл (реком.)	Выкл (реком.)
Режим обучения	Выключен (реком.)	Выключен (реком.)	Выключен (реком.)
Группа "Авторизация сетевых соединений"			
Защита соединений для группы everyone	Да (реком.)	Да (реком.)	–
Обработка сетевых пакетов: Параметры обработки сетевых пакетов	Подпись, Пакет целиком (обяз.)	Подпись, Пакет целиком (обяз.)	–
Обработка сетевых пакетов: Защита от replay-атак	Да (реком.)	Да (реком.)	Да (реком.)
Группа "Контроль устройств"			
Список устройств: Параметры контроля	Параметры заданы, при этом для групп "Устройства USB", включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для групп "Устройства USB", включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для групп "Устройства USB", включен режим "Подключение устройства запрещено" (обяз.)
Список устройств: Разрешения	Заданы (обяз.)	Заданы (обяз.)	Заданы (обяз.)
Группа "Контроль печати"			
Список принтеров: Разрешения	Заданы (обяз.)	Заданы (обяз.)	Заданы (обяз.)

*Действие является обязательным, если для реализации меры ОЦЛ.6 (ограничение прав пользователей по вводу информации в систему) будет применяться механизм полномочного управления доступом системы Secret Net Studio. Если для реализации указанной меры защиты применяются другие решения, действие не обязательно для выполнения.

Параметры пользователей

Для соответствия классам защищенности АСУ ТП должны быть настроены параметры пользователей, перечисленные в следующей таблице. Настройка параметров осуществляется в Центре управления пользователями в диалоговом окне настройки свойств пользователя.

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.22 Параметры пользователей

Параметр	Классы защищенности АСУ ТП		
	К1	К2	К3
Группа параметров "Идентификатор" в диалоге "Параметры безопасности"			
Электронный идентификатор пользователя	Присвоен (обяз.)	Присвоен (реком.)	–
Интеграция с ПАК "Соболь"	Да (реком.)	Да (реком.)	–
Группа параметров "Доступ" в диалоге "Параметры безопасности"			
Уровень допуска	Назначен уполномоченным пользователям (обяз.)*	–	–
Привилегия: Управление категориями конфиденциальности	Назначена уполномоченным пользователям (обяз.)*	–	–

*Действие является обязательным, если для реализации меры ОЦЛ.6 (ограничение прав пользователей по вводу информации в систему) будет применяться механизм полномочного управления доступом системы Secret Net Studio. Если для реализации указанной меры защиты применяются другие решения, действие не обязательно для выполнения.

Параметры механизмов КЦ и ЗПС

Для соответствия классам защищенности АСУ ТП должны быть настроены параметры механизмов КЦ и ЗПС, перечисленные в следующей таблице. Настройка параметров осуществляется в программе "Контроль программ и данных".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.23 Параметры механизмов КЦ и ЗПС

Параметр	Классы защищенности АСУ ТП		
	К1	К2	К3
Диалог "Режимы" в диалоговом окне настройки свойств компьютера			
Режим ЗПС включен	Да (обяз.)	–	–
Мягкий режим	Нет (обяз.)	–	–
Проверять целостность модулей перед запуском	Да (обяз.)	–	–
Проверять заголовки модулей перед запуском	Да (реком.)	–	–
Контролировать исполняемые скрипты	Да (реком.)	–	–
Диалоговое окно настройки параметров задания контроля СЗИ			
Метод контроля ресурсов	Содержимое (обяз.)	Содержимое (обяз.)	–
Алгоритм	CRC32 (реком.)	CRC32 (реком.)	–
Регистрация событий: Успех завершения	Да (реком.)	Да (реком.)	–
Регистрация событий: Ошибка завершения	Да (обяз.)	Да (обяз.)	–
Регистрация событий: Ошибка проверки	Да (обяз.)	Да (обяз.)	–
Реакция на отказ: Действия	Заблокировать компьютер (реком.)	Заблокировать компьютер (реком.)	–
Расписание	При загрузке ОС и по расписанию (обяз.)	При загрузке ОС и по расписанию (обяз.)	–
Диалоговое окно настройки параметров задания контроля ОС (файлы и реестр)			
Метод контроля ресурсов	Содержимое (реком.)	Содержимое (реком.)	–
Алгоритм	CRC32 (реком.)	CRC32 (реком.)	–
Регистрация событий: Успех завершения	Да (реком.)	Да (реком.)	–
Регистрация событий: Ошибка завершения	Да (реком.)	Да (реком.)	–
Регистрация событий: Успех проверки	Нет (реком.)	Нет (реком.)	–
Регистрация событий: Ошибка проверки	Да (реком.)	Да (реком.)	–
Реакция на отказ: Действия	Заблокировать компьютер (реком.)	Заблокировать компьютер (реком.)	–
Расписание	При загрузке ОС и по расписанию (реком.)	При загрузке ОС и по расписанию (реком.)	–

Критическая информационная инфраструктура Российской Федерации

При определенных вариантах настройки система Secret Net Studio обеспечивает соответствие требованиям по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (КИИ), изложенным в нормативном документе "Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации" (утверждены приказом ФСТЭК России от 25 декабря 2017 г. № 239).

Для категорий значимости КИИ ТП К1, К2 и К3 определены базовые наборы мер защиты информации. Организационные и технические меры защиты информации должны обеспечивать реализацию следующих основных требований:

- идентификация и аутентификация;
- управление доступом;
- ограничение программной среды;
- защита машинных носителей информации;
- аудит безопасности;
- антивирусная защита;
- предотвращение вторжений (компьютерных атак);
- обеспечение целостности;
- обеспечение доступности;
- защита технических средств и систем;
- защита информационной (автоматизированной) системы и ее компонентов;
- реагирование на компьютерные инциденты;
- управление конфигурацией;
- управление обновлениями программного обеспечения;
- планирование мероприятий по обеспечению безопасности;
- обеспечение действий в нештатных ситуациях;
- информирование и обучение персонала.

Использование средств доверенной загрузки

В КИИ категорий значимости К1 и К2 должны применяться средства доверенной загрузки операционной системы. В качестве средства доверенной загрузки может использоваться изделие "Программно-аппаратный комплекс "Соболь".

Обеспечение непрерывности функционирования

Для обеспечения непрерывности функционирования Secret Net Studio в КИИ всех категорий значимости рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net Studio

Для соответствия категориям значимости КИИ должны быть настроены параметры политик, перечисленные в следующей таблице. Настройка выполняется в Центре управления на вкладке "Настройки", раздел "Политики".
Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.24 Параметры политик

Параметр	Категории значимости КИИ		
	К1	К2	К3
Группа "Вход в систему"			
Максимальный период неактивности до блокировки экрана	Не более 5 (обяз.)	Не более 15 (реком.)	Не более 15 (реком.)
Запрет вторичного входа в систему	Да (реком.)	Да (реком.)	Да (реком.)
Количество неудачных попыток аутентификации	От 3 до 4 (обяз.)	От 3 до 8 (обяз.)	От 3 до 10 (обяз.)
Время блокировки при достижении количества неудачных попыток аутентификации	От 15 до 60 (обяз.)	От 10 до 30 (обяз.)	От 3 до 30 (обяз.)
Режим идентификации пользователя	Только по идентификатору (обяз.)	Только по идентификатору (реком.)	Смешанный (реком.)
Режим аутентификации пользователя	Усиленная аутентификация по паролю (обяз.)	Усиленная аутентификация по паролю (обяз.)	Усиленная аутентификация по паролю (обяз.)
Парольная политика	Задать свои значения (обяз.)	Задать свои значения (обяз.)	Задать свои значения (обяз.)
Минимальная длина пароля	Не менее 8 символов (обяз.)	Не менее 6 символов (обяз.)	Не менее 6 символов (обяз.)
Срок действия пароля	Не более 60 дней (обяз.)	Не более 90 дней (обяз.)	Не более 120 дней (обяз.)
Сложность пароля	Да (обяз.)	Да (обяз.)	Да (обяз.)
Группа "Журнал"			
Максимальный размер журнала защиты	Не менее 4096 (реком.)	Не менее 4096 (реком.)	Не менее 4096 (реком.)
Политика перезаписи событий	Затирать события по мере необходимости (реком.)	Затирать события по мере необходимости (реком.)	Затирать события по мере необходимости (реком.)
Учетные записи с привилегией просмотра журнала системы защиты	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Учетные записи с привилегией управления журналом системы защиты	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Ключи пользователя"			
Максимальный срок действия ключа	Не более 360 (реком.)	Не более 360 (реком.)	Не более 360 (реком.)
Минимальный срок действия ключа	30 (реком.)	30 (реком.)	30 (реком.)
Предупреждение об истечении срока действия ключа	Не менее 14 (реком.)	Не менее 14 (реком.)	Не менее 14 (реком.)
Группа "Оповещение о тревогах"			
Локальное оповещение о тревогах	Включено (реком.)	Включено (реком.)	Включено (реком.)
Группа "Контроль RDP-подключений"			

Параметр	Категории значимости КИИ		
	К1	К2	К3
Перенаправле- ние устройств в RDP-подключениях	COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.)	COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.)	COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.)
Группа "Контроль административных привилегий"			
Самозащита продукта	Включить (обяз.)	Включить (обяз.)	Включить (обяз.)
Учетные записи с привилегией управления механизмом самозащиты	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Дискреционное управление доступом"			
Учетные записи с привилегией управления правами доступа	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Затирание данных"			
Количество циклов затирания на локальных дисках	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)
Количество циклов затирания на сменных носителях	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)
Количество циклов затирания оперативной памяти	Не менее 2 (обяз.)	–	–
Количество циклов затирания по команде "Удалить безвозвратно"	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)
Количество циклов затирания при уничтожении данных на дисках	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)
Группа "Полномочное управление доступом"			
Названия уровней конфиденциаль-ности	Настроено (обяз.)*	–	–
Режим работы	Контроль потоков включен (обяз.)*	–	–
Режим работы: Строгий контроль терминальных подключений	Да (обяз.)*	–	–
Группа "Замкнутая программная среда"			
Учетные записи, на которые не действуют правила замкнутой программной среды	Локальная группа администраторов (реком.)	–	–
Группа "Межсетевой экран"			
Правила доступа	Настроено (реком.)	Настроено (реком.)	Настроено (реком.)
Протоколы	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)
Включить ICMP-защиту	Да (реком.)	Да (реком.)	–
ICMP-сообщения: Эхо-ответ	Получение (реком.)	Получение (реком.)	–
ICMP-сообщения: Адресат недоступен	Получение, Отправка (реком.)	Получение, Отправка (реком.)	–

Параметр	Категории значимости КИИ		
	К1	К2	К3
ICMP-сообщения: Эхо-запрос	Отправка (реком.)	Отправка (реком.)	–
ICMP-сообщения: Ходатайство маршрутизатора	Получение, Отправка (реком.)	Получение, Отправка (реком.)	–
ICMP-сообщения: Превышение временного интервала	Получение (реком.)	Получение (реком.)	–
ICMP-сообщения: Заблокировать остальные типы	Да (реком.)	Да (реком.)	–
Отслеживать состояние соединений	Вкл (обяз.)	Выкл (реком.)	Выкл (реком.)
Блокировать сетевые пакеты, не соответствующие таблице состояний	Вкл (обяз.)	Выкл (реком.)	Выкл (реком.)
Режим обучения	Выключен (реком.)	Выключен (реком.)	Выключен (реком.)
Группа "Авторизация сетевых соединений"			
Защита соединений для группы everyone	Да (реком.)	Да (реком.)	–
Обработка сетевых пакетов: Параметры обработки сетевых пакетов	Подпись, Пакет целиком (обяз.)	Подпись, Пакет целиком (обяз.)	–
Обработка сетевых пакетов: Защита от replay-атак	Да (реком.)	Да (реком.)	Да (реком.)
Группа "Контроль устройств"			
Список устройств: Параметры контроля	Параметры заданы, при этом для групп "Устройства USB", включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для групп "Устройства USB", включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для групп "Устройства USB", включен режим "Подключение устройства запрещено" (обяз.)
Список устройств: Разрешения	Заданы (обяз.)	Заданы (обяз.)	Заданы (обяз.)
Группа "Контроль печати"			
Список принтеров: Разрешения	Заданы (обяз.)	Заданы (обяз.)	Заданы (обяз.)

*Действие является обязательным, если для реализации меры ОЦЛ.6 (ограничение прав пользователей по вводу информации в систему) будет применяться механизм полномочного управления доступом системы Secret Net Studio. Если для реализации указанной меры защиты применяются другие решения, действие не обязательно для выполнения.

Параметры пользователей

Для соответствия категориям значимости КИИ должны быть настроены параметры пользователей, перечисленные в следующей таблице. Настройка параметров осуществляется в Центре управления пользователями в диалоговом окне настройки свойств пользователя.

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.25 Параметры пользователей

Параметр	Категории значимости КИИ		
	К1	К2	К3
Группа параметров "Идентификатор" в диалоге "Параметры безопасности"			
Электронный идентификатор пользователя	Присвоен (обяз.)	Присвоен (реком.)	–
Интеграция с ПАК "Соболь"	Да (реком.)	Да (реком.)	–
Группа параметров "Доступ" в диалоге "Параметры безопасности"			
Уровень допуска	Назначен уполномоченным пользователям (обяз.)*	–	–
Привилегия: Управление категориями конфиденциальности	Назначена уполномоченным пользователям (обяз.)*	–	–

*Действие является обязательным, если для реализации меры ОЦЛ.6 (ограничение прав пользователей по вводу информации в систему) будет применяться механизм полномочного управления доступом системы Secret Net Studio. Если для реализации указанной меры защиты применяются другие решения, действие не обязательно для выполнения.

Параметры механизмов КЦ и ЗПС

Для соответствия категориям значимости КИИ должны быть настроены параметры механизмов КЦ и ЗПС, перечисленные в следующей таблице. Настройка параметров осуществляется в программе "Контроль программ и данных".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.26 Параметры механизмов КЦ и ЗПС

Параметр	Категории значимости КИИ		
	К1	К2	К3
Диалог "Режимы" в диалоговом окне настройки свойств компьютера			
Режим ЗПС включен	Да (обяз.)	–	–
Мягкий режим	Нет (обяз.)	–	–
Проверять целостность модулей перед запуском	Да (обяз.)	–	–
Проверять заголовки модулей перед запуском	Да (реком.)	–	–
Контролировать исполняемые скрипты	Да (реком.)	–	–
Диалоговое окно настройки параметров задания контроля СЗИ			
Метод контроля ресурсов	Содержимое (обяз.)	Содержимое (обяз.)	–
Алгоритм	CRC32 (реком.)	CRC32 (реком.)	–
Регистрация событий: Успех завершения	Да (реком.)	Да (реком.)	

Параметр	Категории значимости КИИ		
	К1	К2	К3
Регистрация событий: Ошибка завершения	Да (обяз.)	Да (обяз.)	–
Регистрация событий: Ошибка проверки	Да (обяз.)	Да (обяз.)	–
Реакция на отказ: Действия	Заблокировать компьютер (реком.)	Заблокировать компьютер (реком.)	–
Расписание	При загрузке ОС и по расписанию (обяз.)	При загрузке ОС и по расписанию (обяз.)	–
Диалоговое окно настройки параметров задания контроля ОС (файлы и реестр)			
Метод контроля ресурсов	Содержимое (реком.)	Содержимое (реком.)	–
Алгоритм	CRC32 (реком.)	CRC32 (реком.)	–
Регистрация событий: Успех завершения	Да (реком.)	Да (реком.)	–
Регистрация событий: Ошибка завершения	Да (реком.)	Да (реком.)	–
Регистрация событий: Успех проверки	Нет (реком.)	Нет (реком.)	–
Регистрация событий: Ошибка проверки	Да (реком.)	Да (реком.)	–
Реакция на отказ: Действия	Заблокировать компьютер (реком.)	Заблокировать компьютер (реком.)	–
Расписание	При загрузке ОС и по расписанию (реком.)	При загрузке ОС и по расписанию (реком.)	–

Информационные системы, предназначенные для обработки биометрических персональных данных

При определенных вариантах настройки система Secret Net Studio обеспечивает соответствие рекомендациям по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина РФ.

Рекомендации изложены в следующих нормативно-методических документах:

- Указание "О перечне угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 статьи 14.1 Федерального закона от 27 июля 2006 года №149-ФЗ "Об информации, информационных технологиях и о защите информации", в единой биометрической системе (утверждено Центральным Банком Российской Федерации (Банк России) 9 июля 2018 года №4859-У/01/01/782-18);

- Методические рекомендации по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (утверждены Центральным Банком Российской Федерации (Банк России) от 14 февраля 2019 г. № 4-МР);
- Порядок обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядок размещения и обновления биометрических персональных данных в единой биометрической системе, а также требования к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации (утвержден приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 25.06.2018 №321).

Для уровней защиты информации ЕБС-1 (усиленный уровень, для системно значимых кредитных организаций) и ЕБС-2 (стандартный уровень) определены базовые наборы мер защиты информации. Организационные и технические меры защиты информации должны обеспечивать реализацию следующих основных требований:

- идентификация, аутентификация, авторизация;
- управление доступом;
- ограничение программной среды;
- защита машинных носителей информации;
- аудит безопасности;
- антивирусная защита;
- выявление сетевых вторжений и атак;
- сегментация и межсетевое экранирование вычислительных сетей;
- контроль целостности и защищенности;
- защита технических средств и систем;
- защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств;
- управление инцидентами защиты информации;
- защита среды виртуализации.

Использование средств доверенной загрузки

В информационной системе ЕБС всех уровней защиты информации рекомендуется применение средства доверенной загрузки операционной системы в виде аппаратно-программных модулей доверенной загрузки уровня платы расширения, сертифицированных ФСТЭК России на соответствие требованиям к аппаратно-программным модулям доверенной загрузки ЭВМ по 2 классу защиты.

В качестве средства доверенной загрузки может использоваться изделие "Программно-аппаратный комплекс "Соболь".

Обеспечение непрерывности функционирования

Для обеспечения непрерывности функционирования Secret Net Studio в ЕБС всех уровней защиты информации рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net Studio

Для соответствия уровням защиты информации ЕБС должны быть настроены параметры политик, перечисленные в следующей таблице. Настройка выполняется в Центре управления на вкладке "Настройки", раздел "Политики".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.27 Параметры политик

Параметр	Уровень защиты информации ЕБС	
	ЕБС-1	**ЕБС-2**
Группа "Вход в систему"		
Максимальный период неактивности до блокировки экрана	Не более 15 (обяз.)	Не более 15 (реком.)
Запрет вторичного входа в систему	Да (реком.)	Да (реком.)
Время блокировки при достижении количества неудачных попыток аутентификации	Не менее 30 минут (обяз.)	Не менее 30 минут (обяз.)
Режим идентификации пользователя	Только по идентификатору (обяз.)	Только по идентификатору (реком.)
Режим аутентификации пользователя	Усиленная аутентификация по паролю (обяз.)	Усиленная аутентификация по паролю (обяз.)
Парольная политика	Задать свои значения (обяз.)	Задать свои значения (обяз.)
Минимальная длина пароля	Не менее 8 символов (обяз.) Пароль Администратора не менее 16 символов	Не менее 6 символов (обяз.) Пароль Администратора не менее 16 символов
Срок действия пароля	Не более 360 дней (обяз.) Для Администратора не более 90 дней	Не более 360 дней (обяз.) Для Администратора не более 90 дней
Сложность пароля	Да (обяз.)	—
Группа "Журнал"		
Максимальный размер журнала защиты	Не менее 4096 (реком.)	Не менее 4096 (реком.)
Политика перезаписи событий	Затирать события по мере необходимости (реком.)	Затирать события по мере необходимости (реком.)
Учетные записи с привилегией просмотра журнала системы защиты	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Учетные записи с привилегией управления журналом системы защиты	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Ключи пользователя"		
Максимальный срок действия ключа	Не более 360 (реком.)	Не более 360 (реком.)
Минимальный срок действия ключа	30 (реком.)	30 (реком.)
Предупреждение об истечении срока действия ключа	Не менее 14 (реком.)	Не менее 14 (реком.)

Параметр	Уровень защиты информации ЕБС	
	ЕБС-1	**ЕБС-2**
Группа "Оповещение о тревогах"		
Локальное оповещение о тревогах	Включено (реком.)	Включено (реком.)
Группа "Контроль RDP-подключений"		
Перенаправление устройств в RDP-подключениях	COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.)	COM-портов - Запрещено LPT-портов- Запрещено Дисков- Запрещено Устройств Plug and Play- Запрещено подключать удаленные устройства (реком.)
Группа "Контроль административных привилегий"		
Самозащита продукта	все: Включить (обяз.)	все: Включить (обяз.)
Учетные записи с привилегией управления механизмом самозащиты	все: Локальная группа администраторов (реком.)	все: Локальная группа администраторов (реком.)
Группа "Дискреционное управление доступом"		
Учетные записи с привилегией управления правами доступа	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Затирание данных"		
Количество циклов затирания на локальных дисках	Не менее 2 (реком.)	Не менее 1 (реком.)
Количество циклов затирания на сменных носителях	Не менее 2 (реком.)	Не менее 1 (реком.)
Количество циклов затирания оперативной памяти	Не менее 2 (реком.)	Не менее 1 (реком.)
Количество циклов затирания по команде "Удалить безвозвратно"	Не менее 2 (реком.)	Не менее 1 (реком.)
Количество циклов затирания при уничтожении данных на дисках	Не менее 2 (реком.)	Не менее 1 (реком.)
Группа "Полномочное управление доступом"		
Названия уровней конфиденциальности	Настроено (обяз.)	–
Режим работы	Контроль потоков включен (обяз.)	–
Режим работы: Строгий контроль терминальных подключений	Да (обяз.)	–
Группа "Замкнутая программная среда"		
Учетные записи, на которые не действуют правила замкнутой программной среды	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Межсетевой экран"		
Правила доступа	Настроено (реком.)	Настроено (реком.)
Протоколы	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)
Включить ICMP-защиту	Да (реком.)	Да (реком.)
ICMP-сообщения: Эхо-ответ	Получение (реком.)	Получение (реком.)
ICMP-сообщения: Адресат недоступен	Получение, Отправка (реком.)	Получение, Отправка (реком.)
ICMP-сообщения: Эхо-запрос	Отправка (реком.)	Отправка (реком.)

Параметр	Уровень защиты информации ЕБС	
	ЕБС-1	**ЕБС-2**
ICMP-сообщения: Ходатайство маршрутизатора	Получение, Отправка (реком.)	Получение, Отправка (реком.)
ICMP-сообщения: Превышение временного интервала	Получение (реком.)	Получение (реком.)
ICMP-сообщения: Заблокировать остальные типы	Да (реком.)	Да (реком.)
Отслеживать состояние соединений	Вкл (обяз.)	Выкл (реком.)
Блокировать сетевые пакеты, не соответствующие таблице состояний	Вкл (обяз.)	Выкл (реком.)
Режим обучения	Выключен (реком.)	Выключен (реком.)
Группа "Авторизация сетевых соединений"		
Защита соединений для группы everyone	Да (реком.)	Да (реком.)
Обработка сетевых пакетов: Параметры обработки сетевых пакетов	Подпись, Пакет целиком (обяз.)	Подпись, Пакет целиком (обяз.)
Обработка сетевых пакетов: Защита от replay-атак	Да (реком.)	Да (реком.)
Группа "Контроль устройств"		
Список устройств: Параметры контроля	Параметры заданы, при этом для групп "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для групп "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)
Список устройств: Разрешения	Заданы (обяз.)	Заданы (обяз.)
Группа "Контроль печати"		
Список принтеров: Разрешения	Заданы (обяз.)	Заданы (обяз.)

Параметры пользователей

Для соответствия уровням защиты информации ЕБС должны быть настроены параметры пользователей, перечисленные в следующей таблице. Настройка параметров осуществляется в Центре управления пользователями в диалоговом окне настройки свойств пользователя.
Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.28 Параметры пользователей

Параметр	Уровень защиты информации ЕБС	
	ЕБС-1	ЕБС-2
Группа параметров "Идентификатор" в диалоге "Параметры безопасности"		
Электронный идентификатор пользователя	Присвоен (обяз.)	Присвоен (реком.)
Интеграция с ПАК "Соболь"	Да (реком.)	Да (реком.)
Группа параметров "Доступ" в диалоге "Параметры безопасности"		
Уровень допуска	Назначен уполномоченным пользователям (обяз.)	–
Привилегия: Управление категориями конфиденциальности	Назначена уполномоченным пользователям (обяз.)	–

Параметры механизмов КЦ и ЗПС

Для соответствия уровням защиты информации ЕБС должны быть настроены параметры механизмов КЦ и ЗПС, перечисленные в следующей таблице. Настройка параметров осуществляется в программе "Контроль программ и данных".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.29 Параметры механизмов КЦ и ЗПС

Параметр	Уровень защиты информации ЕБС	
	ЕБС-1	ЕБС-2
Диалог "Режимы" в диалоговом окне настройки свойств компьютера		
Режим ЗПС включен	Да (обяз.)	Да (обяз.)
Мягкий режим	Нет (обяз.)	Нет (обяз.)
Проверять целостность модулей перед запуском	Да (обяз.)	Да (обяз.)
Проверять заголовки модулей перед запуском	Да (реком.)	Да (реком.)
Контролировать исполняемые скрипты	Да (реком.)	Да (реком.)
Диалоговое окно настройки параметров задания контроля СЗИ		
Метод контроля ресурсов	Содержимое (обяз.)	Содержимое (обяз.)
Алгоритм	CRC32 (реком.)	CRC32 (реком.)
Регистрация событий: Успех завершения	Да (реком.)	Да (реком.)
Регистрация событий: Ошибка завершения	Да (обяз.)	Да (обяз.)
Регистрация событий: Ошибка проверки	Да (обяз.)	Да (обяз.)
Реакция на отказ: Действия	Заблокировать компьютер (реком.)	Заблокировать компьютер (реком.)
Расписание	При загрузке ОС и по расписанию (обяз.)	При загрузке ОС и по расписанию (обяз.)

Параметр	Уровень защиты информации ЕБС	
	ЕБС-1	**ЕБС-2**
Диалоговое окно настройки параметров задания контроля ОС (файлы и реестр)		
Метод контроля ресурсов	Содержимое (реком.)	Содержимое (реком.)
Алгоритм	CRC32 (реком.)	CRC32 (реком.)
Регистрация событий: Успех завершения	Да (реком.)	Да (реком.)
Регистрация событий: Ошибка завершения	Да (реком.)	Да (реком.)
Регистрация событий: Успех проверки	Нет (реком.)	Нет (реком.)
Регистрация событий: Ошибка проверки	Да (реком.)	Да (реком.)
Реакция на отказ: Действия	Заблокировать компьютер (реком.)	Заблокировать компьютер (реком.)
Расписание	При загрузке ОС и по расписанию (реком.)	При загрузке ОС и по расписанию (реком.)

Применение параметров после настройки

При изменении параметров объектов и защитных механизмов Secret Net Studio не все значения могут вступать в силу сразу после сохранения изменений. Некоторые параметры применяются на защищаемых компьютерах при определенных условиях.

Ниже перечислены параметры, вступающие в силу после перезагрузки компьютера или при следующем входе пользователя в систему. Остальные параметры применяются сразу после сохранения измененных значений.

Табл.30 Параметры в Центре управления

Параметр	Применение
Вкладка "Состояние" для компьютера — средства включения и отключения механизмов	
Дискреционное управление	После перезагрузки
Затирание данных	После перезагрузки
Контроль устройств	После перезагрузки
Замкнутая программная среда	После перезагрузки
Полномочное управление	После перезагрузки
Контроль печати	После перезагрузки
Защита дисков и шифрование	После перезагрузки
Вкладка "Настройки", раздел "Политики" — параметры группы "Вход в систему"	
Максимальный период неактивности до блокировки экрана	При следующем входе в систему
Запрет вторичного входа в систему	После перезагрузки
Запрет смены пользователя без перезагрузки	После перезагрузки
Реакция на изъятие идентификатора	При следующем входе в систему
Количество неудачных попыток аутентификации	При следующем входе в систему
Разрешить интерактивный вход только доменным пользователям	При следующем входе в систему
Режим идентификации пользователя	При следующем входе в систему
Режим аутентификации пользователя	При следующем входе в систему
Парольная политика	При следующем входе в систему
Вкладка "Настройки", раздел "Политики" — параметры группы "Журнал"	
Максимальный размер журнала системы защиты	При увеличении — сразу. При уменьшении — после очистки журнала
Учетные записи с привилегией просмотра журнала системы защиты	При следующем входе в систему
Вкладка "Настройки", раздел "Политики" — параметры группы "Ключи пользователя"	
Все настраиваемые параметры группы	При следующем входе в систему
Вкладка "Настройки", раздел "Политики" — параметры группы "Контроль RDP подключений"	
Перенаправление устройств в RDP-подключениях	При следующем терминальном входе
Перенаправление буфера обмена в RDP-подключениях	При следующем терминальном входе
Перенаправление принтеров в RDP-подключениях	При следующем терминальном входе
Вкладка "Настройки", раздел "Политики" — параметры группы "Администрирование системы защиты"	
Самозащита продукта: Включить	После перезагрузки
Самозащита продукта: Включить контроль административных привилегий	После перезагрузки

Параметр	Применение
Вкладка "Настройки", раздел "Политики" — параметры группы "Дискреционное управление доступом"	
Учетные записи с привилегией управления правами доступа	При следующем входе в систему
Вкладка "Настройки", раздел "Политики" — параметры группы "Полномочное управление доступом"	
Режим скрытия: Скрывать недоступные конфиденциальные файлы	После перезагрузки
Режим скрытия: Отображать недоступные конфиденциальные файлы	После перезагрузки
Режим работы: Контроль потоков отключен	После перезагрузки
Режим работы: Контроль потоков включен	После перезагрузки
Режим работы: Строгий контроль терминальных подключений	При следующем входе в систему
Режим работы: Автоматический выбор максимального уровня сессии	При следующем входе в систему
Вкладка "Настройки", раздел "Политики" — параметры группы "Замкнутая программная среда"	
Учетные записи, на которые не действуют правила замкнутой программной среды	При следующем входе в систему
Вкладка "Настройки", раздел "Политики" — параметры группы "Защита диска и шифрование данных"	
Учетные записи с привилегией на создание криптоконтейнера	При следующем входе в систему
Вкладка "Настройки", раздел "Политики" — параметры группы "Контроль печати"	
Маркировка документов	При следующем входе в систему
Теневое копирование	При следующем входе в систему
Вкладка "Настройки", раздел "Параметры" — параметры группы "Управление трассировкой"	
Все настраиваемые параметры группы	После перезагрузки

Табл.31 Параметры в программе "Контроль программ и данных"

Параметр	Момент применения
Список ресурсов в задании ЗПС	При следующем входе в систему*
Диалоговое окно настройки параметров субъекта управления, диалог "Режимы"	
Режим ЗПС включен	При следующем входе в систему*
Изоляция процесса включена	При следующем входе в систему*

*При централизованной настройке возможно принудительное применение изменений по команде "Перезагрузка параметров работы пользователей" в контекстном меню субъектов управления.

Табл.32 Параметры в Центре управления пользователями

Параметр	Момент применения
Операции с учетными записями: удаление, блокировка, смена пароля	При следующем входе в систему
Окно настройки свойств пользователя, диалог "Параметры безопасности" — параметры группы "Идентификатор"	
Список электронных идентификаторов пользователя	При следующем входе в систему
Окно настройки свойств пользователя, диалог "Параметры безопасности" — параметры группы "Доступ"	
Все параметры полномочного управления доступом	При следующем входе в систему

Открытые порты для работы Secret Net Studio

Для корректного функционирования Secret Net Studio на оборудовании должны быть открыты порты, приведенные в таблицах ниже.

На всех компьютерах и серверах необходимо открыть порты, приведенные в первой таблице данного раздела.

Дополнительно необходимо открыть порты из остальных таблиц данного раздела на оборудовании, выполняющем соответствующие функции.

Табл.33 Открытые порты для всех компьютеров и серверов (общесистемные разрешения для работы с AD)

Назначение	TCP	UDP
Взаимодействие с AD	49152-65535	49152-65535
Взаимодействие с DNS-сервером	49152-65535	53 49152-65535
NetBIOS name resolution	-	137
NetBIOS datagram service	-	138
NTP-синхронизация времени	-	123

Табл.34 Открытые порты для контроллера домена

Назначение	TCP	UDP
Доступ к LDAP	389	389
Доступ к LDAPS	636	-
Механизм GPO, другие взаимодействия с AD	445	-
Служба сеанса NetBIOS	139	-
Kerberos аутентификация пользователя	88	-
RPC-взаимодействия	135	-
Доступ к Global Catalog	3268	-
Доступ к Global Catalog по SSL (если настроен)	3269	-

Табл.35 Открытые порты для других серверов

Назначение	TCP	UDP
DNS-сервер	53	53
SQL-сервер	1433	1434

Табл.36 Открытые порты для сетевого оборудования

Назначение	TCP	UDP
Network broadcast	-	137 138

Табл.37 Открытые порты для работы всех СБ Secret Net Studio

Назначение	TCP	UDP
Интерфейс управления сервера аутентификации	42100	-
Центр распространения ключей Kerberos	42088	42088
Смена пароля пользователя Kerberos	42464	42464
Взаимодействие с Центром управления	443	-
Взаимодействие с Secret Net LDS	50000*	-
Взаимодействие с Secret Net LDS по SSL	50001*	-
Взаимодействие с Secret Net-GC LDS	50002*	-
Взаимодействие с Secret Net-GC LDS по SSL	50003*	-

***** Порт используется по умолчанию, если при установке СБ не указан другой порт.

Табл.38 Открытые порты для работы родительского и подчиненного СБ Secret Net Studio

Назначение	TCP	UDP
RPC-взаимодействия	135	-
Взаимодействие между СБ по HTTP	443	-

Табл.39 Открытые порты для работы СБ, которому подчинен клиент Secret Net Studio

Назначение	TCP	UDP
RPC-взаимодействия	135	-
Взаимодействие СБ и клиента по HTTP	443	-
Автоматическая установка клиента	139	137

Табл.40 Открытые порты для работы клиента Secret Net Studio

Назначение	TCP	UDP
Автоматическая установка клиента с СБ	445	137
RPC-взаимодействие с СБ при централизованной установке клиента	135	-
Аппаратная поддержка	21326	-
Синхронизация настроек механизмов КЦ, ЗПС	21327	-
Согласование ключей ipsec, протокол ISAKMP согласования параметров безопасности	-	42200

ПО для использования поддерживаемых USB-ключей и смарт-карт

Для использования в системе Secret Net Studio поддерживаемых USB-ключей и смарт-карт на компьютере должно быть установлено дополнительное ПО соответствующих производителей устройств. Установку необходимого ПО можно выполнить с установочного диска системы Secret Net Studio. Каталоги с файлами для установки ПО перечислены в следующей таблице.

Тип средства	Каталоги с файлами для установки
USB-ключи и смарт-карты	
Rutoken S, Rutoken ЭЦП, Rutoken Lite	\Tools\Tokens\RuToken\
JaCarta PKI, JaCarta PKI Flash, JaCarta ГОСТ, JaCarta ГОСТ Flash	\Tools\Tokens\Aladdin\JaCartaUC\
eToken PRO (Java)*	\Tools\Tokens\Aladdin\JaCartaUC\ + \Tools\Tokens\Aladdin\eToken\
ESMART Token, ESMART Token ГОСТ	\Tools\Tokens\eSmart\
Считыватели смарт-карт	
Athena ASEDrive	\Tools\Tokens\Aladdin\Acedrv\

* При использовании идентификаторов eToken для работы со стандартными сертификатами Microsoft необходимо дополнительно установить набор драйверов и утилит SafeNet Authentication Client, предоставляемый производителем устройств.

Каталоги установки клиента

При установке клиентского ПО Secret Net Studio создаются четыре системные переменные окружения LocalProtectionDir, NetworkProtectionDir, AntivirusDir и LocalControlCenterDir, в которые записываются пути к каталогам установки клиента и его основных подсистем.

Права доступа на каталог установки клиента наследуются от родительского объекта.

Сведения об установке и настройке СУБД MS SQL

Установку сервера MS SQL необходимо выполнить в соответствии с требованиями производителя. Перечень требований приводится на сайте компании Microsoft.

В частности, перед установкой сервера MS SQL должна быть выполнена установка компонента .NET Framework соответствующей версии и языкового пакета для этого компонента (при использовании русской редакции СУБД).

Общий порядок действий для установки сервера MS SQL с использованием бесплатно распространяемого варианта СУБД (на примере ОС Windows Server 2008 R2 и СУБД версии MS SQL Server 2012 SP1 Express):

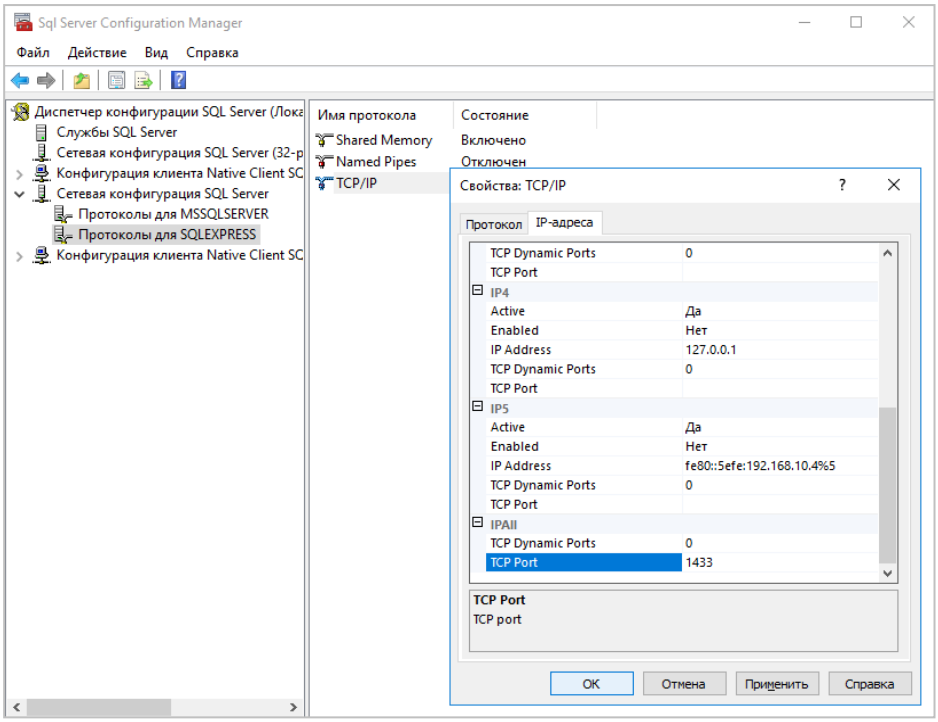
1. Включить в ОС компонент .NET Framework 3.5.
2. Установить .NET Framework 4.5. Для этого запустите на исполнение файл dotNetFx45_Full_x86_x64.exe из каталога \Tools\Microsoft\Prerequisites.
3. Установить языковой пакет к .NET Framework 4.5. Для этого в том же каталоге запустите на исполнение файл dotNetFx45LP_Full_x86_x64ru.exe.
4. Установить сервер MS SQL. Для этого запустите на исполнение файл SQLEXPRWT_x64_ENU.exe или SQLEXPRWT_x86_ENU.exe (в зависимости от разрядности ОС).

Корректное взаимодействие сервера безопасности и СУБД MS SQL обеспечивается при выполнении следующих условий на компьютере сервера MS SQL:

- включен режим поддержки сортировки кириллицы для экземпляра базы данных — для этого при установке экземпляра необходимо в параметрах сортировки для компонента Database Engine указать значение Cyrillic_General_CI_AS (в разделе "Server Configuration", вкладка "Collation");
- включен режим аутентификации, обеспечивающий проверку подлинности SQL Server и Windows, — для этого на сервере MS SQL необходимо включить смешанный режим аутентификации (mixed mode).

Если сервер MS SQL установлен на отдельном компьютере (не на компьютере сервера безопасности), дополнительно требуется выполнить следующие действия:

- в брандмауэре (если он включен) разрешить использование порта для соединения с СУБД (по умолчанию порт 1433). При этом на сервере MS SQL порт должен быть открыт на входящие соединения, а на сервере безопасности — на исходящие;
- включить режим поддержки протокола TCP/IP. Режим по умолчанию отключен при использовании свободно распространяемого варианта SQL Server Express. Управление режимом осуществляется с помощью компонента SQL Server Configuration Manager из состава ПО MS SQL Server. Для включения режима перейдите к разделу "SQL Server Network Configuration / Protocols for <*имя_экземпляра_БД*>" и вызовите окно настройки свойств элемента "TCP/IP". В диалоге "Protocol" укажите значение "Yes" для параметра "Enabled" и затем в диалоге "IP Addresses" проверьте значения параметров "TCP Dynamic Ports" и "TCP Ports" для всех IP-адресов: параметрам должны быть присвоены пустое значение и значение "1433" соответственно. Пример диалога с параметрами настройки представлен на следующем рисунке.



Примечание. При включенной трассировке (см. стр.156) сведения о взаимодействии с СУБД сохраняются на сервере безопасности в log-файлах SnTrace.log и SB.txt (размещаются в каталоге трассировки, по умолчанию это C:\logs). Данные в указанных файлах могут использоваться для диагностики проблем соединения.

Изменения в IIS при установке сервера безопасности

При установке сервера безопасности изменяются некоторые параметры компонентов IIS. Параметрам присваиваются значения, необходимые для корректного функционирования сервера.

В IIS формируется специальный сайт SecretNetStudioSite. Для сайта выполняется:

- установка доступа по SSL;
- привязка (binding) протокола "https" по адресам "*:443:" .

Примечание. Привязка протокола "https" для сайта SecretNetStudioSite добавляется во время установки сервера безопасности, а также при генерации нового сертификата для сервера.
Порт 443 необходим для функционирования сервера безопасности, поэтому для исключения конфликтов при добавлении привязки одновременно удаляются привязки для этого порта на остальных сайтах IIS, развернутых на компьютере. В связи с этим может быть нарушена работоспособность других сайтов и приложений, использующих в IIS порт 443.

В дополнительных параметрах пула приложений SecretNetStudioPool устанавливаются значения для следующих параметров:

Имя параметра	Значение
Раздел (General)	
queueLength	10000
Раздел processModel	
identityType	ApplicationPoolIdentity
idleTimeout	0.00:00:00
pingingEnabled	false
Раздел recycling	
periodicRestart.memory	0
periodicRestart.privateMemory	0
periodicRestart.time	0.00:00:00
periodicRestart.requests	0
periodicRestart.schedule	отключена

В секциях сайтов устанавливаются значения для следующих параметров:

Имя параметра	Значение
Секция сайта system.webServer/serverRuntime	
appConcurrentRequestLimit	100000
uploadReadAheadSize	104857600
Секция сайта windowsAuthentication	
enabled	true
Секция сайта anonymousAuthentication	
enabled	false
Секция сайта handlers	
accessPolicy	Read,Execute

Изменение параметров соединения СБ с БД

Сервер безопасности подключается к базе данных, указанной при установке СБ. При необходимости можно создать новую БД и изменить параметры соединения СБ с БД без переустановки ПО сервера безопасности.

Изменение учетных данных для подключения к БД

Если средствами СУБД были изменены имя и/или пароль учетной записи, используемой для подключения к БД, необходимо внести новые учетные данные в конфигурационный файл СБ. Процедура выполняется на компьютере СБ.

Для изменения учетных данных:

1. В каталоге установленного сервера безопасности запустите утилиту OmsDBPasswordChange.exe через контекстное меню с правами администратора.

   На экране появится окно, представленное на рисунке ниже.

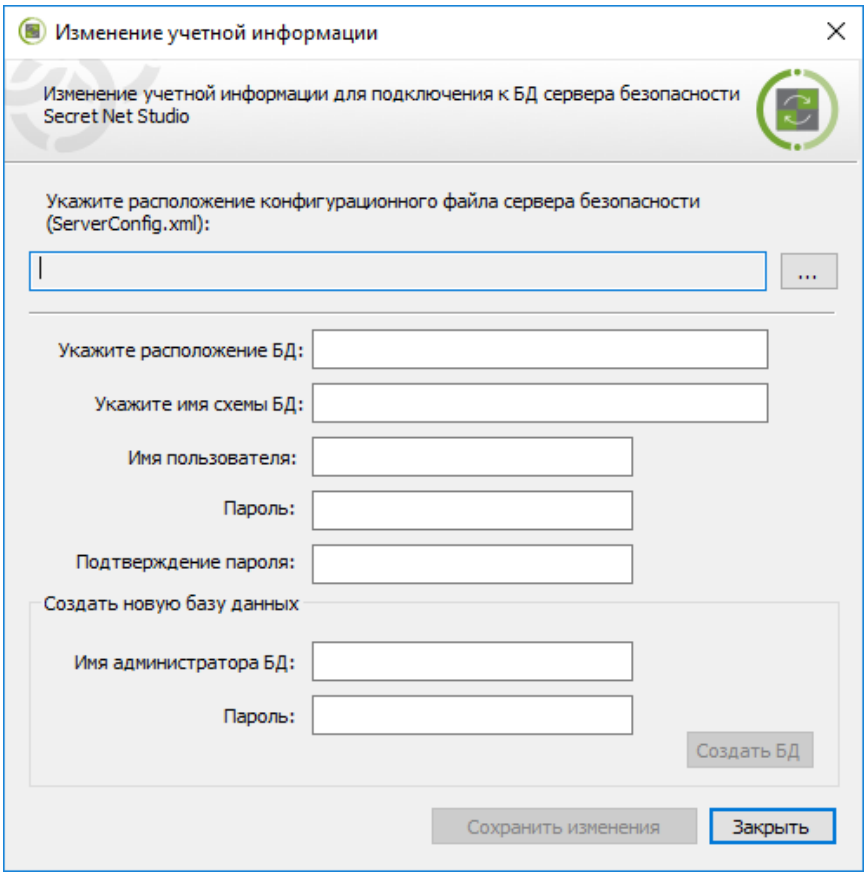


Рис.3 Окно утилиты OmsDBPasswordChange.exe

2. В окне утилиты укажите размещение конфигурационного файла ServerConfig.xml. Для этого нажмите кнопку справа от строки для указания пути и выберите файл в стандартном диалоге ОС Windows.

   Поля с расположением БД, именем схемы БД и именем пользователя для доступа к БД заполнятся автоматически.

3. Введите новые учетные данные пользователя в поля "Имя пользователя", "Пароль" и "Подтверждение пароля".
4. Нажмите кнопку "Сохранить изменения".
5. Перезагрузите компьютер.

Изменение параметров подключения к БД

При необходимости можно изменить параметры подключения СБ к БД:

- имя или IP-адрес компьютера, который является сервером СУБД;
- имя экземпляра БД на этом сервере;
- порт для подключения СБ к БД.

Примечание. Изменение параметров может понадобиться, например, если БД перенесена на другой сервер СУБД. В данном случае необходимо средствами СУБД создать на новом сервере учетную запись для подключения СБ к БД. После создания учетной записи, если ее имя и/или пароль отличаются от предыдущей учетной записи, нужно изменить учетные данные, с которыми СБ выполняет подключение к БД (см. выше).

Для изменения параметров подключения:

1. В каталоге установленного сервера безопасности запустите утилиту OmsDBPasswordChange.exe через контекстное меню с правами администратора.

   На экране появится окно утилиты (см. Рис.3 на стр.**275**).
2. Укажите размещение конфигурационного файла ServerConfig.xml. Для этого нажмите кнопку справа от строки для указания пути и выберите файл в стандартном диалоге ОС Windows.

   Поля с расположением БД, именем схемы БД и именем пользователя для доступа к БД заполнятся автоматически.
3. Измените значение поля с расположением БД, используя следующий формат строки:

   <имя_или_IP-адрес_сервера_MS_SQL>\<имя_экземпляра_БД>,<порт>

   Примечание.
   - Если сервер СУБД установлен на компьютере с СБ и используется стандартное имя экземпляра MSSQLSERVER, то имя или IP-адрес сервера СУБД указывать не нужно.
   - Если для подключения используется порт по умолчанию, то порт можно не указывать.
4. Введите пароль и подтверждение пароля учетной записи, используемой для подключения к БД.
5. Нажмите кнопку "Сохранить изменения".
6. Перезагрузите компьютер.

Создание новой БД

С помощью утилиты OmsDBPasswordChange.exe можно создать новую БД для Secret Net Studio на основе любой БД, имеющейся на сервере СУБД.

Для создания БД:

1. В каталоге установленного сервера безопасности запустите утилиту OmsDBPasswordChange.exe через контекстное меню с правами администратора.

   На экране появится окно утилиты (см. Рис.3 на стр.**275**).
2. Укажите размещение конфигурационного файла ServerConfig.xml. Для этого нажмите кнопку справа от строки для указания пути и выберите файл в стандартном диалоге ОС Windows.

   Поля с расположением БД, именем схемы БД и именем пользователя для доступа к БД заполнятся автоматически.
3. Укажите расположение БД, имеющейся на сервере СУБД, используя следующий формат:

   <имя_или_IP-адрес_сервера_MS_SQL>\<имя_экземпляра_БД>,<порт>

Примечание.
- Если сервер СУБД установлен на компьютере с СБ и используется стандартный экземпляр MSSQLSERVER, то имя или IP-адрес сервера СУБД указывать не нужно.
- Если для подключения используется порт по умолчанию, то порт можно не указывать.

4. Введите имя схемы БД Secret Net Studio, которая будет создана.
5. Введите имя, пароль и подтверждение пароля учетной записи, которая будет использоваться для подключения СБ к БД.
6. В области "Создать новую базу данных" введите учетные данные администратора БД, имеющейся на сервере СУБД.
7. Нажмите кнопку "Создать БД".

   В указанной БД будет создана схема БД Secret Net Studio и учетная запись для подключения СБ к БД.
8. Нажмите кнопку "Сохранить изменения".
9. Перезагрузите компьютер.

Обновление БД

Обновление БД может понадобиться при обновлении Secret Net Studio с версии 8.4 и ниже до актуальной версии.

Внимание! Перед обновлением рекомендуется сделать резервную копию БД средствами СУБД.

Для обновления БД:

1. В каталоге установленного сервера безопасности запустите программу OmsDBPasswordChange.exe через контекстное меню с правами администратора.

   На экране появится окно программы (см. Рис.3 на стр.**275**).
2. Укажите размещение конфигурационного файла ServerConfig.xml. Для этого нажмите кнопку справа от строки для указания пути и выберите файл в стандартном диалоге ОС Windows.

   Поля с расположением БД, именем схемы БД и именем пользователя для доступа к БД заполнятся автоматически.
3. Введите имя, пароль и подтверждение пароля учетной записи, используемой для подключения СБ к БД.

   Примечание. На данном этапе можно создать новую учетную запись для подключения СБ к БД.
4. В области "Создать новую базу данных" введите учетные данные администратора имеющейся БД.
5. Нажмите кнопку "Создать БД".

   На экране появится сообщение "База данных будет обновлена до актуальной версии. Перед процедурой рекомендуется сделать резервную копию".
6. Нажмите кнопку "ОК".

   База данных будет обновлена. Будет создан новый пользователь для подключения СБ к БД.
7. Перезагрузите компьютер.

Особенности использования резервного сервера безопасности

Чтобы обеспечить бесперебойное функционирование защищаемых компьютеров, подчиненных серверу безопасности, следует предусмотреть наличие резервного сервера в этом же домене безопасности. Резервный сервер безопасности должен находиться в постоянной доступности для регулярной синхронизации с основным сервером.

При выходе из строя основного сервера безопасности не происходит автоматического переподчинения компьютеров резервному серверу. Подчинение резервному серверу можно выполнить в Центре управления. Для этого выведите компьютеры из подчинения предыдущему серверу и затем подчините их резервному серверу.

При этом возможны ситуации, когда после переподчинения на компьютерах возникает сбой при определении нового сервера безопасности. Это может происходить из-за недоступности сервера или отсутствия информации о нем в локальном хранилище. Например, если резервный сервер был установлен, а основной сервер вышел из строя в то время, когда компьютер клиента был отключен. В этом случае агент на компьютере не сможет обнаружить новый сервер и из-за этого будет функционировать некорректно. В частности, могут возникнуть проблемы входа в систему в режиме усиленной аутентификации и в других механизмах защиты.

Восстановление некорректно удаленного сервера безопасности

Для функционирования сервера безопасности используются два каталога LDAP: глобальный и доменный. Между этими каталогами выполняется синхронизация, однако в остальном они независимы друг от друга.

Глобальный каталог является единственным для всего леса безопасности, в то же время для каждого домена безопасности в лесу создается свой доменный каталог. Каждый сервер безопасности в лесу относится к единственному глобальному каталогу и к некоторому доменному каталогу, в зависимости от того, в какой домен безопасности он входит.

Перенос ролей мастера схемы и мастера именования LDAP на другой сервер безопасности

В каждом каталоге LDAP (глобальном или локальном) существуют серверы, которым присвоены специальные роли, а именно роль мастера схемы и роль мастера именования, позволяющие выполнять различные операции внутри каталога. По умолчанию обе роли присваиваются первому серверу в каталоге (в случае глобального каталога это первый сервер в лесу безопасности, в случае доменного каталога – первый сервер в домене).

Если по какой-либо причине компьютер, которому присвоены роли, недоступен, то некоторые операции внутри каталога буду невозможны.

Для исправления ситуации необходимо восстановить доступность сервера или выполнить перенос ролей мастера схемы и мастера именования на другой сервер безопасности.

Примечание. В общем случае в каталоге LDAP разные роли могут быть присвоены разным серверам – мастером схемы может являться один сервер, а мастером именования другой. Однако для корректного функционирования серверов безопасности необходимо, чтобы обе роли принадлежали одному серверу безопасности как в глобальном, так и в доменном каталоге. При переносе ролей необходимо следить за тем, чтобы в рамках леса в глобальном каталоге один сервер являлся как мастером схемы, так и мастером именования. Также в рамках каждого домена некоторый сервер безопасности должен являться и мастером схемы, и мастером именования доменного каталога.

Дальнейшие операции описаны с учетом того, что обе роли присвоены одному серверу.

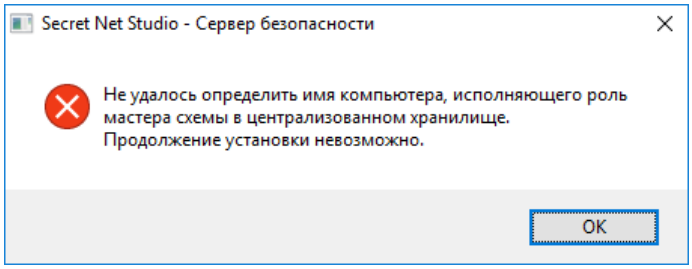
Причины недоступности мастера схемы

Выделяют две основные причины, по которым мастер схемы может оказаться недоступен в глобальном или локальном каталоге:

1. Сервер безопасности, выполняющий роль мастера схемы, был удален из леса или домена безопасности. По умолчанию мастером схемы в глобальном каталоге является первый сервер в лесу. Аналогично, мастером схемы в локальном каталоге является первый сервер в домене безопасности. Если удалить первый сервер в лесу, то такой лес потеряет мастера схемы глобального каталога. Если в некотором домене удалить первый сервер в домене, то такой домен потеряет мастера схемы доменного каталога.
2. Сервер безопасности, выполняющий роль мастера схемы, был потерян (например, машина была физически отключена от сети и больше никогда не включалась) или некорректно удален (без ввода паролей администраторов домена и леса безопасности, в результате чего информация о сервере осталась в каталоге). В этом случае каталог через некоторое время диагностирует, что мастер схемы длительное время не выходил на связь, и будет считать, что мастер схемы отсутствует.

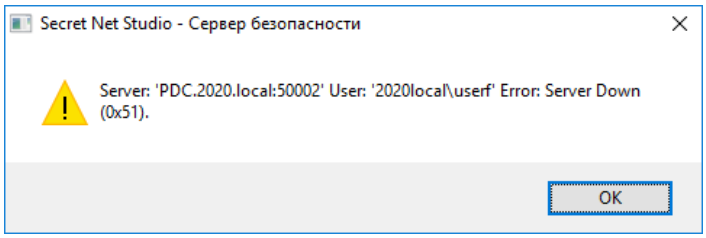
Проблемы, возникающие при отсутствии мастера схемы

Если мастер схемы глобального каталога был удален, то при установке новых серверов безопасности в данный лес может появляться следующая ошибка:



Аналогично, если в некотором домене безопасности в его доменном каталоге удален мастер схемы, то при попытке установить новый сервер безопасности в данный домен может появляться вышеуказанная ошибка.

Если сервер мастера схемы глобального или доменного каталога был потерян по какой-либо причине (не существует, был некорректно удален), то в процессе установки нового сервера появится следующая ошибка:



Просмотр ролей в глобальном и доменном каталогах

Для того чтобы выяснить, какой сервер является мастером схемы и мастером именования, можно воспользоваться утилитой Dsmgmt, входящей в состав ОС Windows:

1. На компьютере, на котором установлена серверная версия ОС Windows, запустите консоль командной строки (cmd.exe) от имени администратора леса (если планируется просмотр ролей в глобальном каталоге) или от имени администратора домена (если планируется просмотр ролей в доменном каталоге).
2. Введите команду запуска утилиты:
   ```
   dsmgmt
   ```
3. В появившейся строке **dsmgmt:** введите команду управления:
   ```
   roles
   ```
4. В появившейся строке **fsmo maintenance:** введите команду управления:
   ```
   connections
   ```
5. В появившейся строке **server connections:** введите команду управления:
   ```
   connect to server <имя_компьютера>:<номер_порта>
   ```
6. В параметрах команды укажите полное DNS-имя компьютера сервера безопасности, принадлежащего лесу, если нужно просмотреть роли в лесу (или принадлежащего интересующему домену безопасности, если нужно просмотреть роли в конкретном доменном каталоге) и номер порта (значение порта по умолчанию для глобального каталога равно 50002, для доменного каталога — 50000).
7. После соединения с указанным компьютером в строке **server connections:** введите команду:
   ```
   quit
   ```
8. В строке **fsmo maintenance:** введите команду управления:
   ```
   select operation target
   ```
9. В строке **select operation target:** введите команду управления:
   ```
   list roles for connected server
   ```

В результате выполнения вышеуказанной команды на экран будет выведено сообщение примерно следующего содержания:

```
Server "pdc:50002" knows about 2 roles
Schema - CN=NTDS Settings\0ADEL:98e3bb5c-8645-400f-8436-
8905e8c53b54,CN=2016FD$SecretNet-GC\0ADEL:8098b33f-16ec-44fa-
85d9-ff74aacea953,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,CN={00D201E5-F194-489D-9A9C-
6B28E33C2ADE}
Naming Master - CN=NTDS Settings\0ADEL:98e3bb5c-8645-400f-
8436-8905e8c53b54,CN=2016FD$SecretNet-GC\0ADEL:8098b33f-16ec-
44fa-85d9-ff74aacea953,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,CN={00D201E5-F194-489D-9A9C-
6B28E33C2ADE}
```

Данное сообщение содержит приставку DEL и имя сервера. Это значит, что сервер удален.

В системном журнале службы ADAM (Secretnet-GC) будет зарегистрировано следующее событие:

```
Event ID 2091: Ownership of the following FSMO role is set to
a server which is deleted or does not exist. Operations which
require contacting a FSMO operation master will fail until
this condition is corrected.
```

В случае если мастер схемы не был удален или же он был потерян (вся информация о сервере осталась в системе), результат вывода команды **list roles for connected server** будет примерно следующим:

```
Server "pdc:50002" knows about 2 roles
Schema - CN=NTDS Settings,CN=BOSS$SecretNet-
GC,CN=Servers,CN=Default-First-Site-N
ame,CN=Sites,CN=Configuration,CN={20256F81-63B0-46B4-991C-
74AC57F17622}
Naming Master - CN=NTDS Settings,CN=BOSS$SecretNet-
GC,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,CN={20256F81-63B0-
46B4-991C-74AC57F176
22}
```

Данное сообщение не содержит пометок DEL напротив имен серверов, исполняющих роли мастера схемы и мастера именования.

Перенос ролей

Перенос ролей выполняется с помощью утилиты Dsmgmt из состава ОС Windows.

Внимание! После переноса ролей мастера схемы и мастера именования на другой компьютер будет утрачена возможность использования в этом качестве для предыдущего компьютера. Поэтому перенос ролей необходимо выполнять только в случае невозможности восстановления функционирования этого сервера. Если сервер безопасности, с которого были перенесены роли (пока он был недоступен) снова появится в лесу (или домене безопасности), это приведет к нарушению работоспособности, так как в каталоге LDAP будет более одного сервера с данными ролями.

Для переноса ролей мастера схемы и мастера именования LDAP:

1. На компьютере сервера безопасности, который будет использоваться в качестве мастера схемы и мастера именования, запустите консоль командной строки (cmd.exe) от имени администратора леса (если планируется перенос ролей в глобальном каталоге) или от имени администратора домена (если планируется перенос ролей в доменном каталоге).
2. Введите команду запуска утилиты:

   ```
   dsmgmt
   ```

3. В появившейся строке **dsmgmt:** введите команду управления:

```
roles
```

4. В появившейся строке **fsmo maintenance:** введите команду управления:

```
connections
```

5. В появившейся строке **server connections:** введите команду управления:

```
connect to server <имя_компьютера>:<номер_порта>
```

В параметрах команды укажите полное DNS-имя компьютера сервера безопасности, который будет использоваться в качестве мастера схемы (или значение **localhost**), и номер порта (значение порта по умолчанию для глобального каталога равно 50002, для доменного каталога — 50000).

6. После соединения с указанным компьютером в строке **server connections:** введите команду:

```
quit
```

7. В строке **fsmo maintenance:** введите команду управления:

```
seize schema master
```

8. По появившейся информации о результате выполнения команды убедитесь, что роль мастера схем присвоена нужному серверу безопасности.
9. В строке **fsmo maintenance:** введите команду управления:

```
seize naming master
```

10. По появившейся информации о результате выполнения команды убедитесь, что роль мастера именования присвоена нужному серверу безопасности.
11. После присвоения ролей мастера схемы и мастера именования завершите работу с утилитой с помощью команды **quit**.

Параметры сетевого взаимодействия

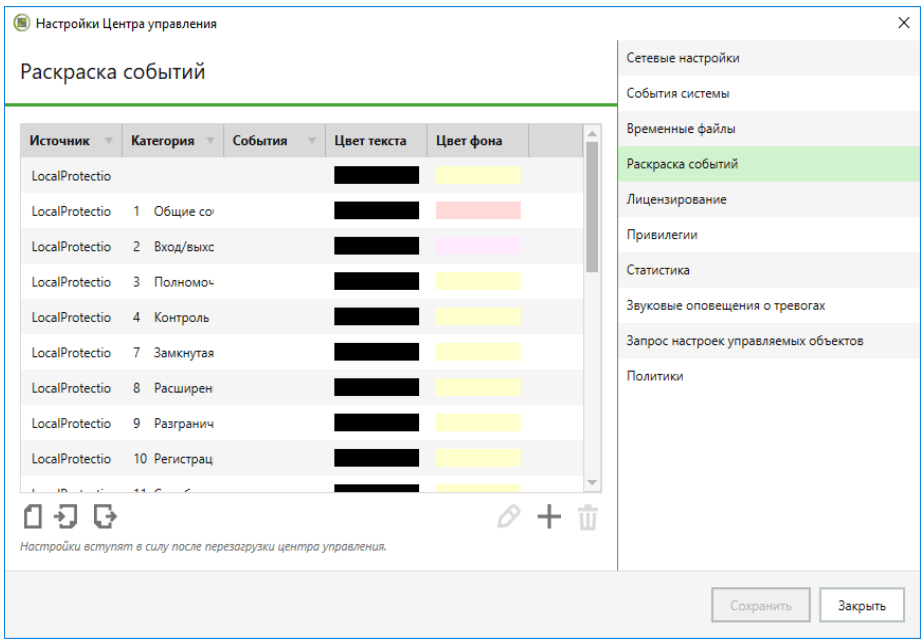
Наименование параметра, пояснение	Значения
Группа параметров "Время ожидания"	
Разрешения имени DNS	30–1000 с
Соединения с сервером	30–1000 с
Отправки запроса на сервер	30–1000 с
Окончания передачи следующего блока Определяет временной интервал, в течение которого ожидается подтверждение о доставке или сообщение об ошибке доставки блока. Параметр предназначен для корректного отслеживания времени жизни операций, связанных с передачей потоковых данных по сети. Определяется пропускной способностью сети: чем она выше, тем меньше может быть временной интервал. В случае уменьшения значения параметра до недопустимого уровня корректная работа транспортной подсистемы может быть нарушена. Ускорить работу транспортной подсистемы параметр не может	30–1000 с
Событий для рабочей станции Определяет промежуток времени, через который сервером отправляется контрольный запрос. Параметр предназначен для контроля соединения. Принцип контроля основан на периодической отправке служебного запроса и получении ответа на него. В случае получения корректного ответа соединение считается работающим. При получении некорректного ответа или по истечении времени ожидания ответа (см. следующий параметр) соединение считается отключенным. При увеличении значения параметра теряется оперативность получения достоверной информации о состоянии соединения	30–1000 с
Сервером ответа на контрольный запрос Определяет максимальное время ожидания ответа на отправленный контрольный запрос. Параметр предназначен для контроля установленного соединения	30–1000 с
Группа параметров "Размер блока"	

Наименование параметра, пояснение	Значения
Для приема данных от сервера Определяет размер буфера транспортной подсистемы для приема потоковых данных. Параметр предназначен для оптимизации процесса передачи по сети потоковой информации. Его значение определяется пропускной способностью сети: чем она выше, тем больше может быть размер буфера	48–10240 Кб
Для передачи данных на сервер Параметр предназначен для оптимизации процесса передачи по сети потоковой информации. Его значение определяется пропускной способностью сети: чем она выше, тем больше может быть размер блока	48–10240 Кб
Группа параметров "Переподключение"	
Включить переподключение Определяет, будет ли производиться автоматическое переподключение к серверу безопасности в случае неудачи подключения и в случае потери соединения с сервером. Если данный параметр отключен, то подключение к серверу после потери соединения выполняется вручную	Вкл/Выкл
Интервал между попытками переподключения Определяет промежуток времени, через который производится повторная попытка автоматического переподключения к серверу безопасности после потери соединения с сервером или в случае неудачи подключения	30–1000 с
Параметр "Обновление конфигурации"	
Параметр может принимать одно из следующих значений: • **Ручное. По кнопке "Обновить конфигурацию"**; • **Автоматическое. По событию об изменении конфигурации**	

Параметры цветового оформления записей журналов

При настройке параметров работы Центра управления (см. стр.**123**) можно сформировать список правил, определяющих цвет текста и фона отображаемых записей журналов в зависимости от заданных условий. Список правил представлен в группе "Раскраска событий" диалога настройки параметров.

Пример списка правил представлен на рисунке ниже.

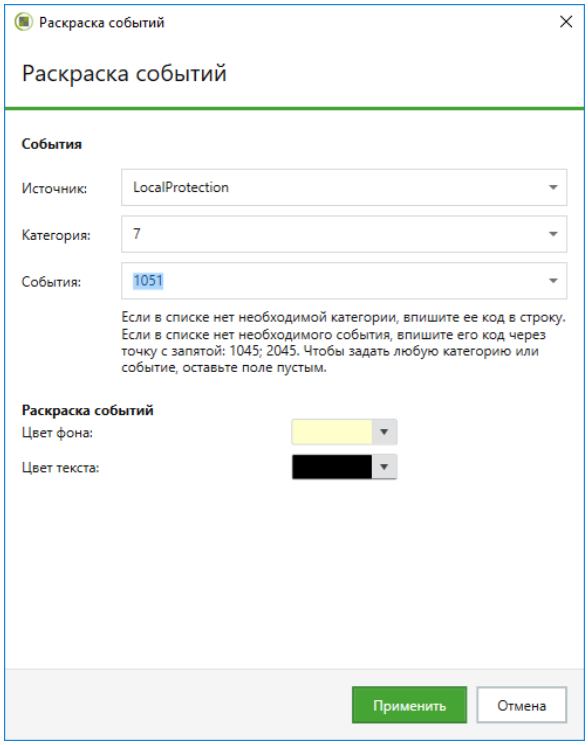


Управление списком правил осуществляется с помощью кнопок, расположенных под списком:

Кнопка	Описание
Взять значения по умолчанию	Возвращает исходный список правил, используемый по умолчанию
Импортировать	Загружает список правил, сохраненный в файле
Экспортировать	Сохраняет текущий список правил в файле
Редактировать	Вызывает диалоговое окно для настройки параметров выбранного правила (см. ниже)
Добавить	Добавляет новое правило в список. Для нового правила выполняется настройка параметров в диалоговом окне (см. ниже)
Удалить	Удаляет выбранный элемент из списка

Настройка параметров правила

Пример диалогового окна настройки параметров правила представлен на рисунке ниже.



Для настройки параметров правила:

1. В группе полей "События" настройте параметры анализа событий:

Источник
Содержит имя компонента или подсистемы, которое указывается при регистрации событий в качестве источника. Выберите нужный источник
Категория
Содержит числовой код категории событий. Выберите код нужной категории из раскрывающегося списка или введите значение вручную. Список категорий, доступных для выбора, формируется в зависимости от указанного источника
События
Содержит числовые идентификаторы событий. Выберите идентификаторы нужных событий из раскрывающегося списка или введите значение вручную. Список событий, доступных для выбора, формируется в зависимости от указанной категории. Несколько идентификаторов разделяются символом ";"

Примечание. Сведения о событиях можно получить при просмотре записей журнала на вкладке "Общее" (см. стр.191). Источники, коды категорий и идентификаторы событий представлены, соответственно, в следующих полях вкладки: "Источник", "Код категории" и "Событие".

2. В группе полей "Раскраска событий" настройте параметры цветового оформления фона и текста строк в таблице записей. Для вызова средств изменения цвета нажмите кнопку в правой части поля.
3. Нажмите кнопку "Применить".

Восстановление журналов из архивов

Записи централизованных журналов, помещенные в архив из БД сервера безопасности, могут быть снова восстановлены в базе данных сервера с помощью Центра управления. Восстановленные записи могут быть загружены для просмотра так же, как и другие записи, хранящиеся в БД.

Внимание! Выполнять восстановление архивов может только пользователь, которому предоставлена привилегия "Архивирование/восстановление журналов".

Для восстановления записей из архива:

1. В диаграмме управления или в списке объектов вызовите контекстное меню сервера безопасности, раскройте подменю "Архивирование" и выберите команду "Восстановить архив журналов".

   На экране появится диалог, содержащий список доступных для восстановления архивов.

2. Выберите нужный архив, журналы (если архив содержит несколько журналов) и нажмите кнопку "Восстановить".

Рекомендации по обслуживанию СУБД для сервера безопасности

Основной причиной снижения производительности сервера безопасности является неправильное или несвоевременное выполнение регламентных процедур в СУБД MS SQL Server (SQL-сервер). Сервер безопасности работает с нагрузкой и обслуживает одновременно большое количество клиентов. Настроенные автоматические действия, выполняемые SQL-сервером, недостаточны для эффективной работы сервера безопасности.

Для увеличения производительности сервера безопасности необходимо автоматизировать процесс выполнения регламентных процедур, используя встроенные средства SQL-сервера. Рекомендуется регулярно выполнять и контролировать следующие регламентные процедуры:

- дефрагментация и реиндексация индексов;
- обновление статистик;
- резервное копирование базы данных;
- архивирование журналов.

Дефрагментация и реиндексация индексов

Для ускорения обработки запросов к БД сервера безопасности на SQL-сервере автоматически создаются специальные объекты — индексы. Индексы содержат сведения для поиска по массивам в базе данных.

В процессе эксплуатации сервера безопасности содержимое базы данных меняется. Наиболее объемные изменения в БД связаны, как правило, с обработкой централизованных журналов. В частности, после архивирования журналов высвобождается часть отведенной памяти в базе данных. Эти изменения со временем могут приводить к фрагментации данных, что в свою очередь повлияет на производительность сервера.

Чтобы поддерживать нормальный режим работы базы данных, рекомендуется регулярно запускать процедуру дефрагментации/реиндексации индексов на SQL-сервере (в среднем достаточно одного раза в неделю). Процедура дефрагментации/реиндексации индексов не требует остановки функционирования сервера, однако для оптимального выполнения рекомендуется запускать команду в моменты наименьшей нагрузки.

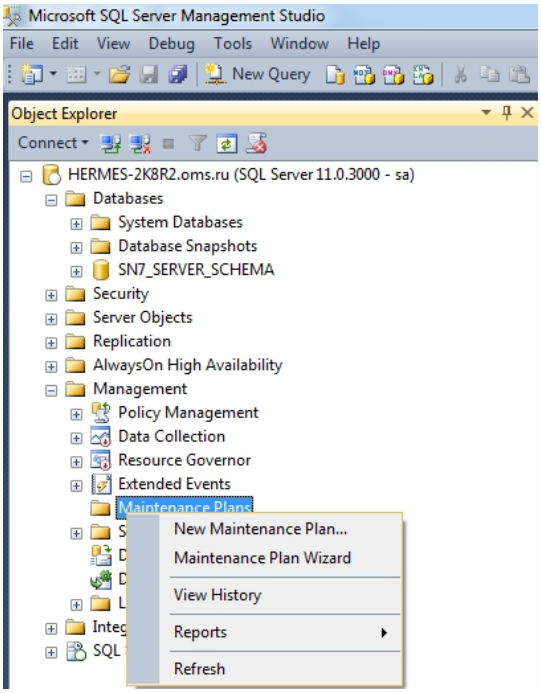
Для дефрагментации/реиндексации индексов можно использовать файл, прилагаемый на установочном диске комплекта поставки системы Secret Net Studio. Перед использованием файла выполните следующие действия:

1. На SQL-сервере создайте каталог на локальном диске.
2. Скопируйте в него с установочного диска содержимое каталога \Tools\SecurityCode\ClearMSSQL\.

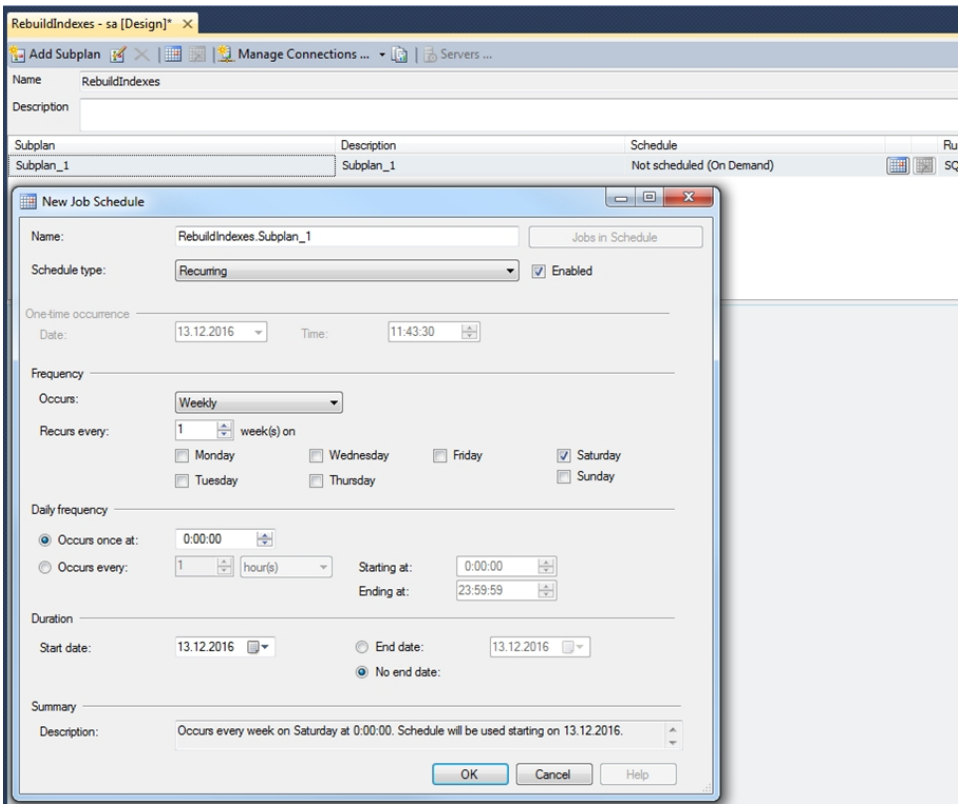
После этого запустите на исполнение файл rebuild_index.sql во время наименьшей загруженности SQL-сервера. Для запуска файла в определенный момент можно использовать заранее созданный план обслуживания.

Для создания плана обслуживания:

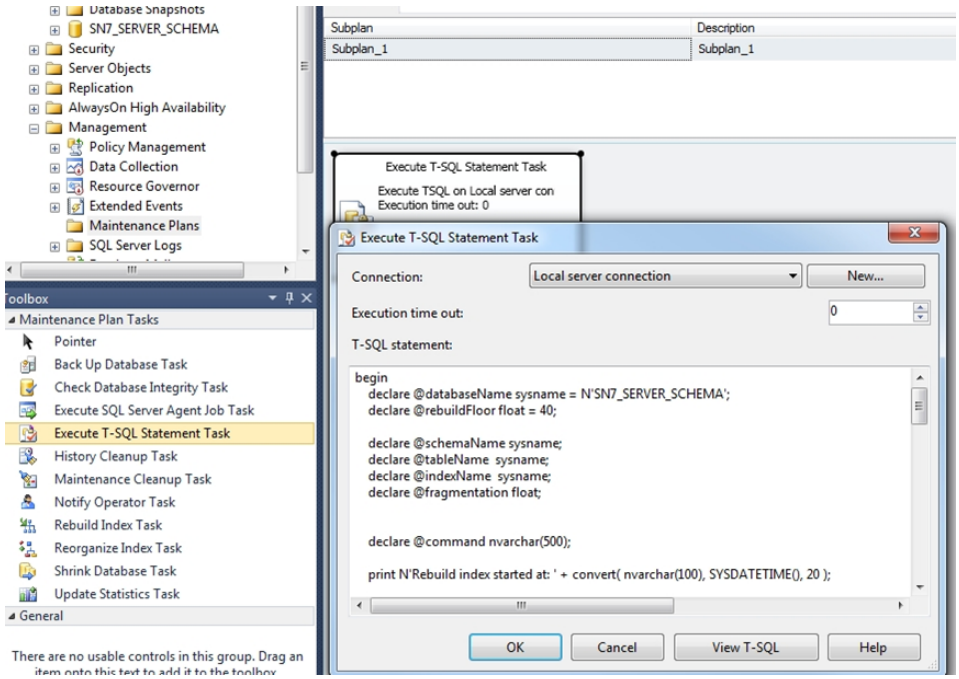
1. Откройте MS SQL Server Management Studio.
2. В окне структуры раскройте ветвь дерева "Management".
3. Вызовите контекстное меню объекта "Maintenance Plans" и выберите команду "New Maintenance Plan...".



4. Настройте расписание запуска плана обслуживания.



5. Перенесите из панели инструментов "Toolbox" элемент "Execute T-SQL Statement Task" и настройте его, скопировав содержимое файла rebuild_index.sql в поле "T-SQL Statement:".



6. Для завершения изменений нажмите кнопку "OK".

При использовании SQL-сервера Express-редакции необходимо создать периодическое задание в планировщике заданий Windows на запуск командного файла со следующим содержанием:

```
osql.exe -d [имя_схемы_БД] -i rebuild_index.sql
```

где *[имя_схемы_БД]* – имя схемы БД Secret Net Studio.

Пример:

```
osql.exe -d SN7_SERVER_SCHEMA -i rebuild_index.sql
```

Примечание. Запуск задания осуществляется от пользователя, входящего в группу администраторов SQL-сервера.

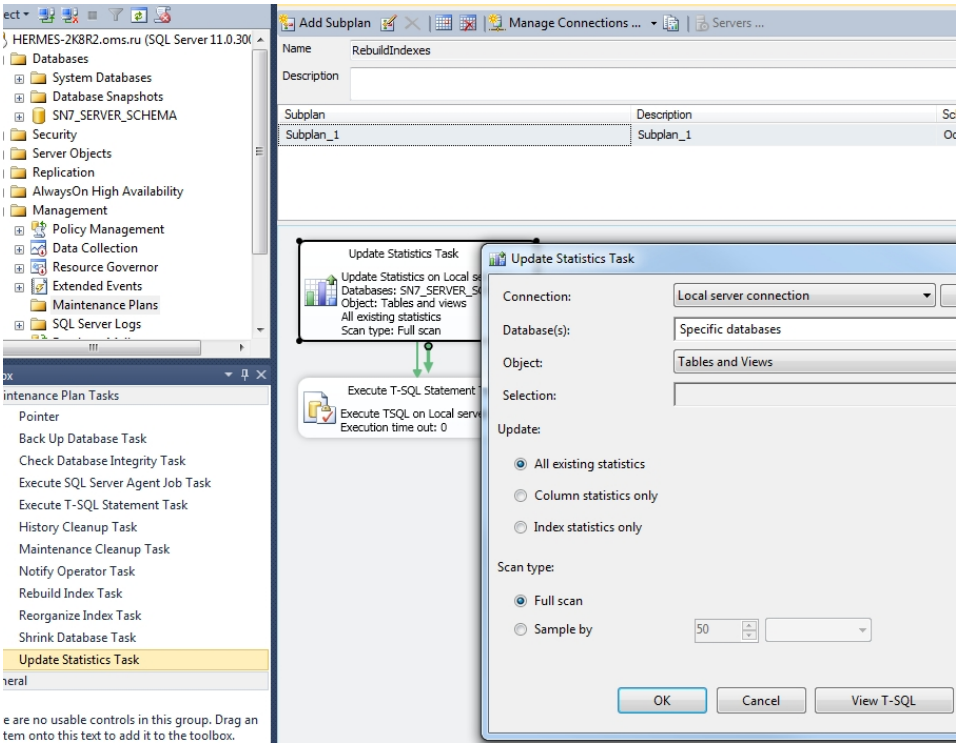
Обновление статистик

SQL-сервер формирует план запроса на основании статистической информации о распределении значений в индексах и таблицах. Статистическая информация собирается на основании образца данных. Автоматическое обновление происходит при изменении образца данных. Иногда этого недостаточно SQL-серверу для стабильного построения оптимального плана выполнения всех запросов.

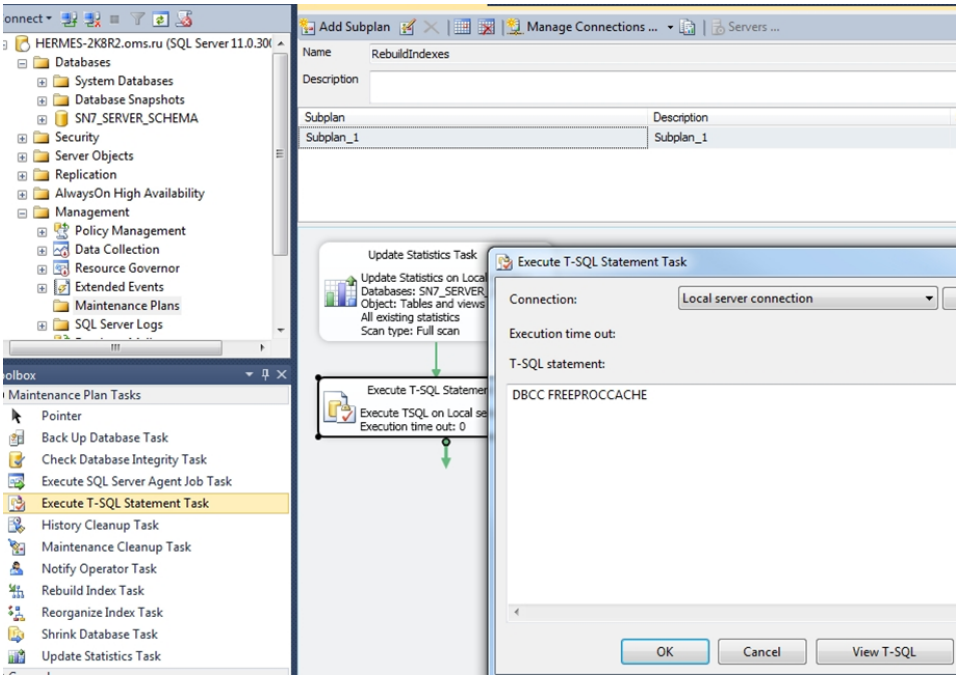
Для гарантии правильной работы SQL-сервера рекомендуется регулярно запускать процедуру обновления статистик базы данных (в среднем достаточно одного раза в день). Процедура обновления статистик базы данных не требует остановки функционирования сервера, однако для оптимального выполнения рекомендуется запускать команду в моменты наименьшей нагрузки.

Для создания плана обновления статистик:

1. Откройте MS SQL Server Management Studio.
2. В окне структуры раскройте ветвь дерева "Management".
3. Вызовите контекстное меню объекта "Maintenance Plans" и выберите команду "New Maintenance Plan...".
4. Настройте расписание запуска: один раз в сутки в полночь.
5. Перенесите из панели инструментов "Toolbox" элемент "Update Statistics Task" и настройте его.



6. Добавьте в план задание на сброс кеша хранимых процедур, переместив из панели инструментов "Toolbox" элемент "Execute T-SQL Statement Task", и в поле "T-SQL Statement:" добавьте команду "DBCC FREEPROCCACHE".



7. Для завершения изменений нажмите кнопку "OK".

При использовании SQL-сервера Express-редакции необходимо создать периодическое задание в планировщике заданий Windows на запуск командного файла со следующим содержанием:

```
osql.exe -d SN7_SERVER_SCHEMA -i update_statistic.sql
```

Содержимое файла update_statistics.sql должно быть следующим.

```
USE SN7_SERVER_SCHEMA;
EXEC sp_msforeachtable N'UPDATE STATISTICS ? WITH FULLSCAN';
GO
DBCC FREEPROCCACHE;
GO
```

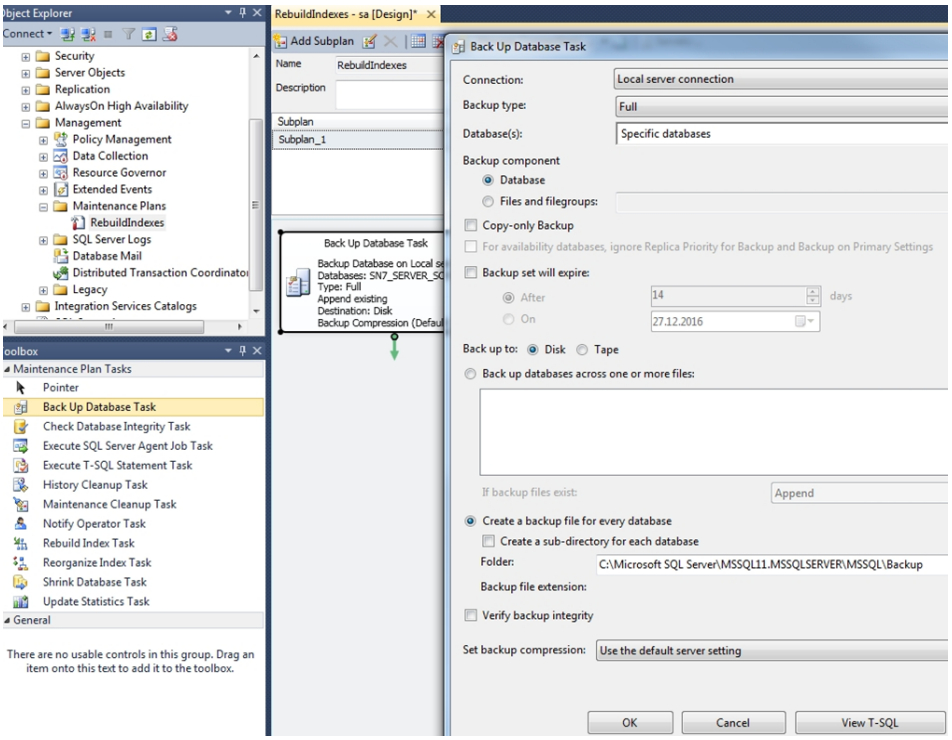
Примечание. Запуск задания осуществляется от пользователя, входящего в группу администраторов SQL-сервера.

Резервное копирование базы данных

Для восстановления базы данных в случае сбоя необходимо создать план резервного копирования. Рекомендуется делать полную резервную копию базы данных (в среднем достаточно одного раза в неделю) и журнала транзакций (в среднем достаточно одного раза в день).

Для создания плана полной резервной копии базы данных:

1. Откройте MS SQL Server Management Studio.
2. В окне структуры раскройте ветвь дерева "Management".
3. Вызовите контекстное меню объекта "Maintenance Plans" и выберите команду "New Maintenance Plan...".
4. Настройте расписание запуска: один раз в неделю.
5. Перенесите из панели инструментов "Toolbox" элемент "Back Up Database Task" и настройте его, выбрав тип резервной копии "Full" и базу "SN7_SERVER_SCHEMA".

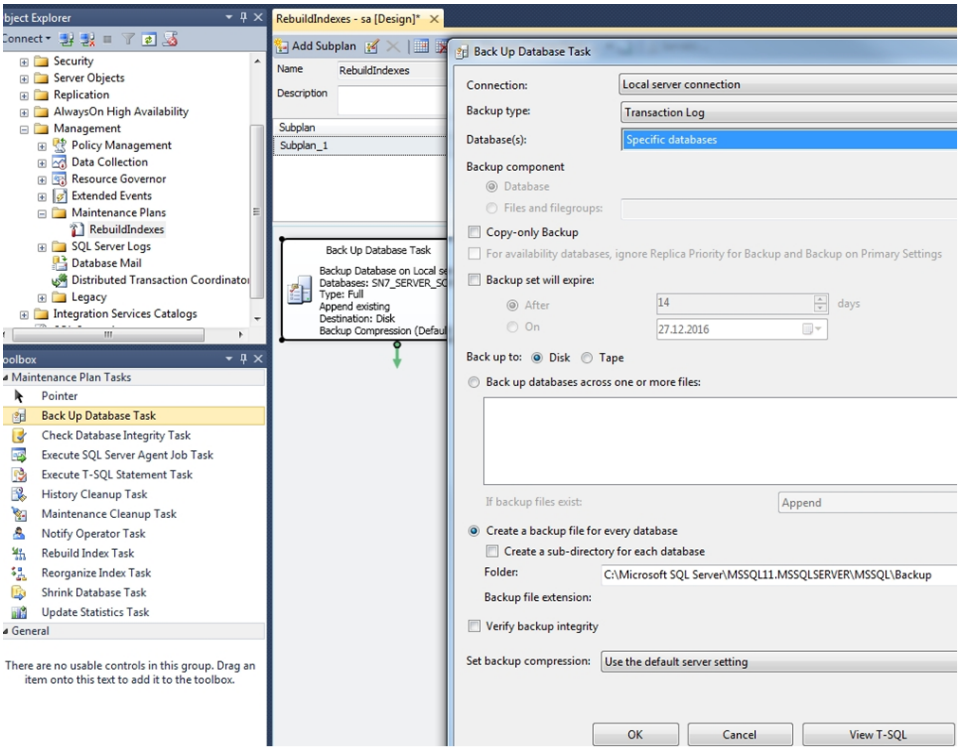


6. Для завершения изменений нажмите кнопку "OK".

Для создания плана резервной копии журнала транзакций:

1. Откройте MS SQL Server Management Studio.
2. В окне структуры раскройте ветвь дерева "Management".
3. Вызовите контекстное меню объекта "Maintenance Plans" и выберите команду "New Maintenance Plan...".
4. Настройте расписание запуска: один раз в неделю.

5. Перенесите из панели инструментов "Toolbox" элемент "Back Up Database Task" и настройте его, выбрав тип резервной копии "Transaction Log" и базу "SN7_SERVER_SCHEMA".



6. Для завершения изменений нажмите кнопку "OK".

При использовании SQL-сервера Express-редакции необходимо создать два периодических задания в планировщике заданий Windows для создания резервной копии всей базы данных и резервной копии журнала транзакций.

Для создания резервной копии всей базы данных содержание командного файла должно быть следующим:

```
osql.exe -d SN7_SERVER_SCHEMA -q "BACKUP DATABASE SN7_SERVER_
SCHEMA TO DISK='C:\SN7_SERVER_Data.bak'"
```

Путь к файлу C:\SN7_SERVER_Data.bak следует заменить на реальный путь к файлу с резервной копией.

Для создания резервной копии журнала транзакций данных содержание командного файла должно быть следующим:

```
osql.exe -d SN7_SERVER_SCHEMA -q "BACKUP LOG SN7_SERVER_
SCHEMA TO DISK='C:\SN7_SERVER_Log.bak'"
```

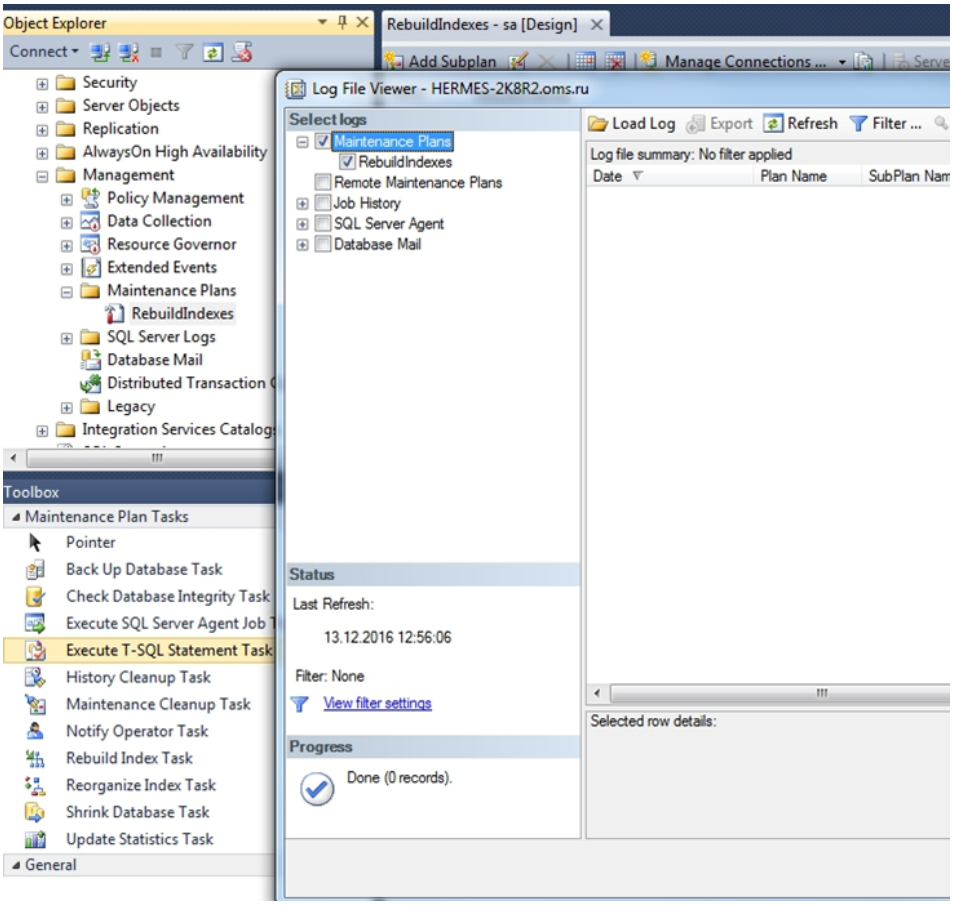
Путь к файлу C:\SN7_SERVER_Log.bak следует заменить на реальный путь к файлу с резервной копией.

Примечание. Запуск заданий осуществляется от пользователя, входящего в группу администраторов SQL-сервера.

Регулярный контроль выполнения планов обслуживания базы данных обеспечивает увеличение производительности сервера безопасности.

Для проверки выполнения созданного плана обслуживания базы данных:

1. Откройте MS SQL Server Management Studio.
2. В окне структуры раскройте ветвь дерева "Management".
3. Вызовите контекстное меню объекта "Maintenance Plans" и выберите команду "View History".



4. Для завершения просмотра нажмите кнопку "Close".

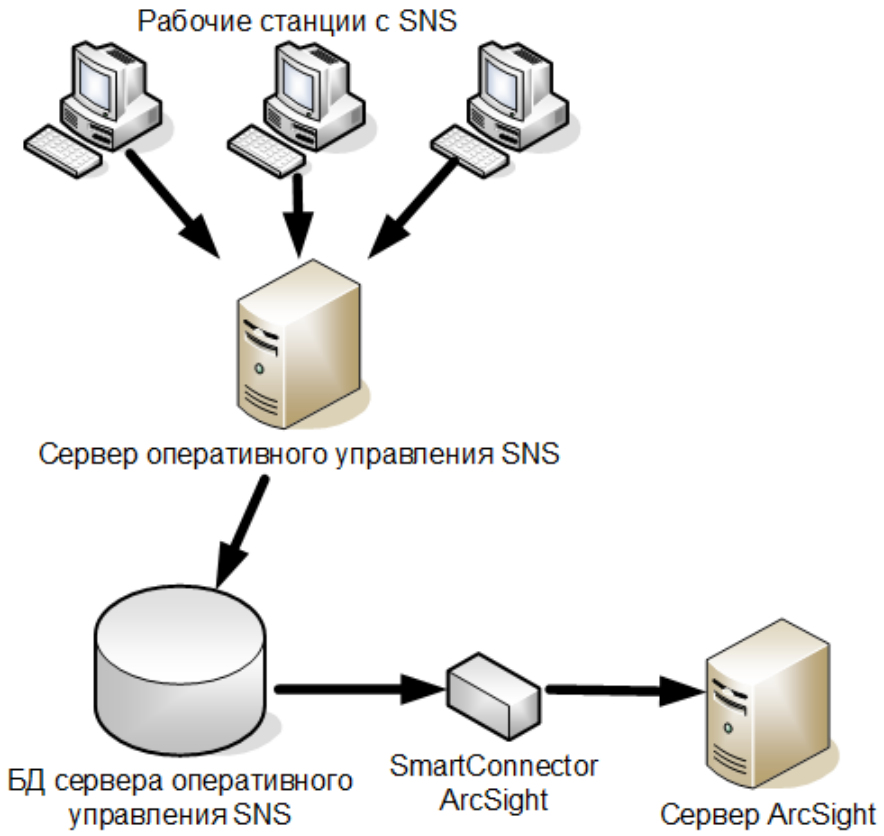
Архивирование журналов

Для SQL-сервера Express-редакции актуальна процедура архивирования журналов (см. стр.**191**). При превышении ограничения на объем базы данных сервер безопасности оказывается в нерабочем состоянии. Расписание архивирования настраивается из расчета 100 МБ на одного клиента в день. Пространство базы данных для одного клиента зависит от количества событий тревог и частоты сбора журналов.

Интеграция Secret Net Studio с SIEM-системами

Имеется возможность интеграции Secret Net Studio с SIEM-системами. По мере сбора журналов Secret Net Studio с рабочих станций данные могут быть оперативно предоставлены SIEM-системе из БД, работающей под управлением СУБД MS SQL Server.

Схема потоков данных при интеграции на примере SIEM-системы ArcSight представлена на рисунке ниже.



Для интеграции Secret Net Studio с SIEM-системой необходимо выполнить следующие действия:

- настроить чтение журналов из БД MS SQL Server для Secret Net Studio (можно использовать представление данных ниже);
- настроить соединение, адаптер или уведомления для SIEM-системы.

Пояснение. Для настройки соединения обратитесь к документации на используемую SIEM-систему.

Для настройки чтения журналов из БД MS SQL Server для Secret Net Studio:

1. Создайте представление (view) с помощью следующего SQL-скрипта.

Внимание!

- Указанный ниже скрипт актуален для Secret Net Studio версий 8.2 и выше. Скрипт для более ранних версий приведен в документации на соответствующие версии продукта.
- Указанный ниже скрипт не отрабатывает на Secret Net Studio версии 8.6, если отсутствует таблица SERVICE.
- Указанный ниже скрипт не отрабатывает на Secret Net Studio версии 8.8, если отсутствуют таблицы SERVICE T2, SERVICEPROVIDER T3.

```
/*
your DB name instead of "SN7_SERVER_SCHEMA"
*/

USE [SN7_SERVER_SCHEMA]
GO

EXEC sp_configure 'clr enabled' , '1';
RECONFIGURE;
GO
/*
creates stored function and view
*/

/*
load dll
*/

/* Beware!
drops function and assembly if it exists to avoid name collision
*/

IF OBJECT_ID('dbo.GetDescription') IS NOT NULL
        DROP FUNCTION dbo.GetDescription;
GO
IF (select top 1 count(x.[name]) from
(select
        a.[name]
        from sys.assembly_files f
full outer join sys.assemblies a
        on f.assembly_id=a.assembly_id
full outer join sys.assembly_modules m
        on a.assembly_id=m.assembly_id
) as x where [name] like '%ByteDataToDeviceInfoConverterAsm') = 1
DROP ASSEMBLY ByteDataToDeviceInfoConverterAsm
GO

IF EXISTS (SELECT 1
                FROM SYSOBJECTS
                WHERE ID = OBJECT_ID('SECRETNETLOG')
                AND TYPE = 'V')
        DROP VIEW SECRETNETLOG
GO

CREATE ASSEMBLY ByteDataToDeviceInfoConverterAsm
FROM 'C:\CLRDeviceInfoConverter\DBConverter.dll';
GO
```

```
/*
create function from assembly
*/

CREATE FUNCTION dbo.GetDescription (@data varbinary (max), @eventid int,@eventmessage
nvarchar(max), @locale nvarchar(5))
RETURNS nvarchar(max)
AS EXTERNAL NAME
[ByteDataToDeviceInfoConverterAsm].
[ByteDataToDeviceInfoConverter.CLRConverter].[GetDescription];
GO



/****** Object: View [dbo].[SERVICEEVENTLOGS] Script Date: 13.11.2018 11:24:41 ******/
SET ANSI_NULLS ON
GO

SET QUOTED_IDENTIFIER ON
GO
/*-
================================================-
===============*//* View: SECRETNETLOG
don't forget to set locale at dbo.GetDescription(E.DATA, E.EVENTID, "ru-RU");
possible locales are: en-US, ru-RU, es-ES;

*/
/*-
================================================-
===============*/
CREATE VIEW SECRETNETLOG ( ID, TIMEWRITTEN, STATION, CATEGORY, EVENTID, EVENTMESSAGE, TYPE,
COMPUTER, USERSID, USERDOMAINNAME, USERNAME )
AS
SELECT T.EVENTLOGRECID,
        T.TIMEWRITTEN,
        C.MNAME,
        CAST (T.CATEGORYMESSAGE as nvarchar(512)),
        T.EVENTID,
        CAST (dbo.GetDescription(T.DATA, T.EVENTID, T.EVENTMESSAGE ,'ru-RU') as nvarchar(MAX)),
        T.TYPEDESCRIPTION,
        T.COMPUTERNAME,
        T.USERSID,
        T.USERDOMAINNAME,
        T.USERNAME
FROM EVENTLOGREC T INNER JOIN CLIENT C on T.CLIENTID = C.CLIENTID
WHERE T.EVENTLOGTYPE=4
```

GO

2. Укажите путь к поставляемому файлу DBConverter.dll в блоке:
   CREATE ASSEMBLY ByteDataToDeviceInfoConverterAsm
   FROM 'C:\CLRDeviceInfoConverter\DBConverter.dll';
   GO
   Также по этому пути должна находиться библиотека ResourceClassLibrary.dll.
3. Укажите требуемую локализацию ('en-US', 'ru-RU', 'es-ES') в строке:
   CAST (dbo.GetDescription(T.DATA, T.EVENTID, 'ru-RU') as nvarchar(1024))

Информация о колонках созданного представления приведена в таблице ниже.

Имя колонки	Тип данных	Макс. размер	Назначение
ID	Int	–	Служебный идентификатор события
TIMEWRITTEN	Дата/время	–	Время возникновения события
STATION	Строка	255 байт	Имя рабочей станции, с которой получен журнал
CATEGORY	Строка	512 байт	Категория события
EVENTID	Int	–	Идентификатор события
EVENTMESSAGE	Строка	2 Гбайт	Описание события
TYPE	Строка	255 байт	Тип события
COMPUTER	Строка	128 байт	Компьютер, который вызвал наступление события (соответствует полю "Компьютер" в стандартном LogViewer)
USERSID	Строка	128 байт	SID пользователя
USERDOMAINNAME	Строка	128 байт	Домен пользователя
USERNAME	Строка	128 байт	Имя пользователя

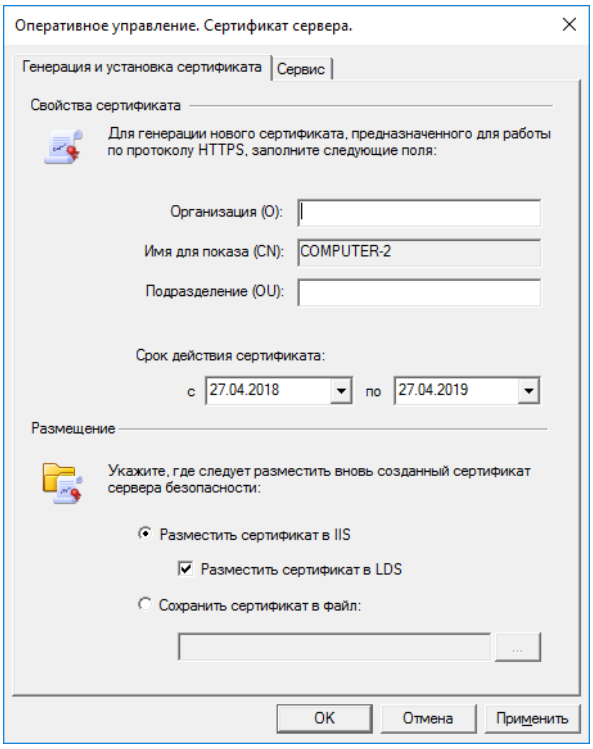
Генерация и установка сертификата сервера безопасности

Процедура выполняется на компьютере сервера безопасности.

Для генерации и установки нового сертификата СБ:

1. В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Сертификаты".

   На экране появится диалоговое окно настройки:



2. В группе полей "Свойства сертификата" укажите нужные значения.

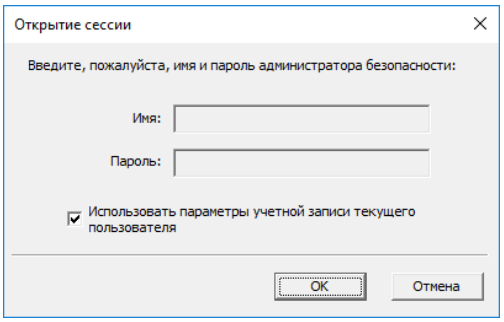
   Примечание. Поля "Организация" и "Подразделение" необязательны для заполнения.

3. В группе полей "Размещение" укажите места размещения сертификата и нажмите кнопку "Применить".

   При наличии в IIS установленного ранее сертификата на экране появится запрос на продолжение записи нового сертификата.

4. Нажмите кнопку "ОК" в диалоге запроса.

   На экране появится диалог:



5. Укажите учетные данные пользователя, имеющего права на запись в хранилище объектов централизованного управления, и нажмите кнопку "ОК".

Пояснение. Если текущий пользователь имеет права на запись — отметьте поле "Использовать параметры учетной записи текущего пользователя". Если права не предоставлены — введите данные соответствующей учетной записи. По умолчанию правами на запись в хранилище обладают пользователи, входящие в группу администраторов домена безопасности.

После установки нового сертификата на экране появится сообщение об этом.

Сведения о настройке защищенного соединения со службами каталогов

В системе Secret Net Studio предусмотрен режим усиленной защиты доступа к хранилищу объектов централизованного управления Secret Net Studio. В этом режиме сетевые обращения к службам AD LDS, выполняемые компонентами системы Secret Net Studio, осуществляются с использованием протоколов SSL/TLS. Данные протоколы предусматривают проверку подлинности компьютера, на котором развернута служба каталогов (сервер безопасности), и реализуют функции установления безопасного соединения с использованием сертификатов.

Для использования режима усиленной защиты в системе должна быть организована и настроена инфраструктура открытых ключей (PKI). Реализация PKI может обеспечиваться стандартными средствами ОС Windows или ПО сторонних производителей. Ниже в данном разделе приводятся общие сведения о порядке организации и настройки PKI с применением стандартных средств ОС.

Защита взаимодействия с AD LDS

Для защиты взаимодействия со службами AD LDS настройка PKI выполняется в следующем порядке:

1. В доверенном центре сертификации (Certification Authority, ЦС) запросите сертификат для сервера безопасности. Для сертификата необходимо указать полное доменное имя компьютера сервера безопасности и метод использования "Проверка подлинности сервера" (Server Authentication). Полученный сертификат импортируйте в хранилище в контексте компьютера, раздел "Личное" (или "Личные").

   Примечание. Если в системе отсутствует ЦС, для организации защищенных соединений можно использовать самозаверенный сертификат, созданный на сервере безопасности. Этот сертификат в дальнейшем применяется и как сертификат компьютера, и как сертификат ЦС.

2. Установите полученный сертификат в IIS. Для этого запустите диспетчер служб IIS (IIS Manager) и в зависимости от версии ОС выполните соответствующие действия:
   - В иерархическом списке раскройте раздел сайтов, вызовите контекстное меню элемента "SecretNetStudioSite" и выберите команду "Изменить привязки" (Edit Bindings).
   - В появившемся списке привязок сайта вызовите диалог настройки для элемента с типом "https" и выберите полученный сертификат в списке SSL-сертификатов.
   - После установки сертификата выполните перезапуск IIS с помощью соответствующей команды управления в контекстном меню элемента "SecretNetStudioSite".
3. Предоставьте необходимые разрешения для доступа к файлу ключа сертификата. Для этого в программе Проводник перейдите к каталогу по умолчанию, в котором хранятся ключи. Местоположение каталога в ОС Windows Server 2012: %ProgramData%\Microsoft\Crypto\RSA\MachineKeys. В других версиях ОС: %ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\RSA \MachineKeys. В каталоге вызовите окно настройки свойств файла ключа сертификата (определить нужный файл в списке можно по дате и времени создания), перейдите на вкладку "Безопасность" и добавьте в список нужную учетную запись с разрешениями по умолчанию. Имя добавляемой учетной записи зависит от того, на каком компьютере установлен сервер безопасности:
   - если СБ установлен на контроллере домена — учетная запись с именем OMS_LDS_xxx$;
   - если СБ установлен на любом другом компьютере — учетная запись с именем NETWORK SERVICE.

4. На компьютере сервера безопасности импортируйте сертификат сервера в раздел "Личное" (или "Личные") хранилищ в контексте экземпляров служб SecretNet и SecretNet-GC. Для этого загрузите оснастку "Сертификаты" в режиме управления сертификатами компьютера и в режиме управления сертификатами каждой службы (т. е. загружаются три оснастки). Выполните экспорт сертификата сервера вместе с закрытым ключом из раздела "Личное" (или "Личные") оснастки с сертификатами компьютера и затем импорт в разделы "ADAM_SecretNet\Личное" и "ADAM_SecretNet-GC\Личное" (или "ADAM_SecretNet\Личные" и "ADAM_SecretNet-GC\Личные") оснасток с сертификатами служб. После этого предоставьте разрешения для доступа к файлам ключей импортированных сертификатов (см. действие **3**).
5. Если имеется еще один сервер безопасности, выполните перечисленные выше действия применительно к этому серверу.
6. Загрузите Центр управления сертификатами сервера безопасности (с помощью элемента "Сертификаты" в разделе основного меню "Код Безопасности") и выполните синхронизацию сертификата, установленного в IIS, с сертификатом сервера безопасности. Для этого в диалоговом окне настройки перейдите на вкладку "Сервис" и нажмите кнопку "Синхронизировать".
7. Откройте конфигурационный файл ServerConfig.xml, который размещается в каталоге установки сервера безопасности. Найдите параметр UseSSLConnection и измените значение false на true. В параметре Name (расположен ниже) измените значение на полное доменное имя компьютера сервера безопасности. Сохраните изменения и перезагрузите компьютер.
8. Для включения шифрования на компьютерах, подчиненных серверу безопасности, установите на них сертификат сервера безопасности и корневой сертификат в хранилище в контексте компьютера:
   - сертификат сервера безопасности установите в раздел "Личное" (или "Личные");
   - корневой сертификат установите в раздел "Доверенные корневые центры сертификации".
9. Включите режим усиленной защиты трафика на защищаемых компьютерах. Для этого в Центре управления выберите нужные объекты в панели "Компьютеры", перейдите на вкладку "Состояние" и включите параметр "Шифровать управляющий сетевой трафик". Параметр начнет действовать на компьютерах после их перезагрузки.

События, регистрируемые в журнале сервера безопасности

Табл.41 События всех категорий сервера безопасности

Название	ID	Описание
Установлено соединение с сервером	1	Установлено соединение между рабочей станцией и сервером безопасности. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • ID сессии
Завершено соединение с сервером	2	Завершено соединение между рабочей станцией и сервером безопасности. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • ID сессии

Название	ID	Описание
Отказ в установке соединения	3	Произошел отказ в установлении соединения между рабочей станцией и сервером безопасности. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • ID сессии; • причина отказа
Запрос конфигурации оперативного управления	4	Отправлен запрос на получение конфигурации оперативного управления
Ошибка получения конфигурации оперативного управления	6	Во время получения конфигурации оперативного управления произошла ошибка. Описание ошибки указано в поле "Описание"
Изменение конфигурации оперативного управления	7	Изменена конфигурация оперативного управления. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • создано объектов; • изменено объектов; • удалено объектов; • обновлена конф. МСЭ; • удаление конф. МСЭ; • изменены настройки: (сбор журналов: <SID пользователей>,архивирование: <SID пользователей>, почтовая рассылка о тревогах: <SID пользователей>, сетевые настройки: <SID пользователей>)
Ошибка изменения конфигурации оперативного управления	8	Во время изменения конфигурации оперативного управления произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • создано объектов; • изменено объектов; • удалено объектов; • обновлена конф. МСЭ; • удаление конф. МСЭ; • изменены настройки: (сбор журналов: <SID пользователей>,архивирование: <SID пользователей>, почтовая рассылка о тревогах: <SID пользователей>, сетевые настройки: <SID пользователей>); • описание ошибки
Выполнение команды	10	Запущен процесс выполнения команды. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • команда; • агенты

Название	ID	Описание
Ошибка выполнения команды	12	Во время запущенного процесса выполнения команды произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • команда; • агенты; • описание ошибки
Запрос на архивирование журналов	13	Отправлен запрос на архивирование содержимого журналов в базе данных сервера безопасности. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • типы журналов; • описание; • временная отсечка
Запрос на архивирование журналов выполнен	14	Отправленный запрос на архивирование содержимого журналов в базе данных сервера безопасности выполнен. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • типы журналов; • описание; • временная отсечка
Ошибка архивирования журналов	15	Во время архивирования содержимого журналов в базе данных сервера безопасности произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • типы журналов; • описание; • временная отсечка; • описание ошибки
Началось архивирование журналов по расписанию	16	Запущен процесс архивирования содержимого журналов в базе данных сервера безопасности согласно установленному расписанию. В поле "Описание" указываются: • типы журналов; • описание; • временная отсечка
Архивирование журналов по расписанию выполнено	17	Процесс архивирования содержимого журналов в базе данных сервера безопасности, согласно установленному расписанию, выполнен. В поле "Описание" указываются: • типы журналов; • описание; • временная отсечка

Название	ID	Описание
Ошибка архивирования журналов по расписанию	18	Во время процесса архивирования содержимого журналов в базе данных сервера безопасности, согласно установленному расписанию, произошла ошибка. В поле "Описание" указываются: • типы журналов; • описание; • временная отсечка; • описание ошибки
Запрос на восстановление журналов из архива	19	Отправлен запрос на восстановление содержимого журналов в базе данных сервера безопасности из архива. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • типы журналов
Запрос на восстановление журналов из архива выполнен	20	Отправленный запрос на восстановление содержимого журналов в базе данных сервера безопасности из архива выполнен. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • типы журналов
Ошибка восстановления журналов из архива	21	Во время восстановления содержимого журналов в базе данных сервера безопасности из архива произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • типы журналов; • описание ошибки
Оповещения о тревогах успешно загружены на сервер	23	Успешная загрузка оповещений о событиях тревоги на сервер безопасности. В поле "Описание" указываются: • компьютер; • SID компьютера; • UAID (уникальный идентификатор блока НСД, под которым блок сохранен в СУБД); • количество оповещений
Ошибка при загрузке оповещений о тревогах на сервер	24	Во время загрузки оповещений о событиях тревоги на сервер безопасности произошла ошибка. В поле "Описание" указываются: • компьютер; • SID компьютера; • UAID (уникальный идентификатор блока НСД, под которым блок сохранен в СУБД); • количество оповещений; • описание ошибки
Получен журнал с рабочей станции	25	Загружен журнал с рабочей станции в базу данных сервера безопасности. В поле "Описание" указываются: • компьютер; • SID компьютера; • типы журналов

Название	ID	Описание
Ошибка получения журнала с рабочей станции	26	Во время загрузки журнала с рабочей станции в базу данных сервера безопасности произошла ошибка. В поле "Описание" указываются: • компьютер; • SID компьютера; • типы журналов; • описание ошибки
Журнал получен для просмотра	27	Журнал загружен в базу данных сервера безопасности для просмотра его содержимого. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • тип журнала; • запрос
Ошибка получения журнала для просмотра	28	Во время загрузки журнала в базу данных сервера безопасности для просмотра его содержимого произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • тип журнала; • запрос; • описание ошибки
Инициирование процедуры получения журнала (ов)	29	Автоматическое включение процедуры загрузки журнала(ов) в базу данных сервера безопасности. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • тип журнала; • запрос
Начало сбора журналов	30	Запущен процесс сбора журналов в базу данных сервера безопасности. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • агенты; • типы журналов
Сбор журналов успешно завершен	31	Запущенный процесс сбора журналов в базу данных сервера безопасности успешно завершен. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • агенты; • типы журналов

Название	ID	Описание
Ошибка при сборе журналов	32	Во время сбора журналов в базу данных сервера безопасности произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • агенты; • типы журналов; • описание ошибки
Начат сбор журналов по расписанию	33	Запущен процесс сбора журналов в базу данных сервера безопасности согласно установленному расписанию. В поле "Описание" указываются: • компьютер; • SID компьютера; • агенты; • типы журналов
Сбор журналов по расписанию успешно завершен	34	Запущенный процесс сбора журналов в базу данных сервера безопасности, согласно установленному расписанию, успешно завершен. В поле "Описание" указываются: • компьютер; • SID компьютера; • агенты; • типы журналов
Ошибка при сборе журналов по расписанию	35	Во время сбора журналов в базу данных сервера безопасности, согласно установленному расписанию, произошла ошибка. В поле "Описание" указываются: • компьютер; • SID компьютера; • агенты; • типы журналов; • описание ошибки
Изменена конфигурация ОУ	36	Изменена конфигурация оперативного управления. В поле "Описание" указываются: • компьютер; • SID компьютера; • список идентификаторов измененных объектов управления: агентов и серверов
Ошибка при изменении конфигурации ОУ	37	Во время изменения конфигурации оперативного управления произошла ошибка. В поле "Описание" указываются: • компьютер; • SID компьютера; • список идентификаторов измененных объектов управления: агентов и серверов; • описание ошибки
Квитирование тревог	38	Подтверждение приема событий тревог. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • квитирование; • уровни угроз: (низкий| повышенный| высокий) или идентификаторы:<список идентификаторов квитируемых тревог>; • комментарий

Название	ID	Описание
Ошибка при квитировании тревог	39	Во время подтверждения событий тревог произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • квитирование; • уровни угроз: (низкий| повышенный| высокий) или идентификаторы:<список идентификаторов квитируемых тревог>; • комментарий; • описание ошибки
Ошибка при подключении к вышестоящему серверу	40	Во время подключения к вышестоящему серверу безопасности произошла ошибка. В поле "Описание" указываются: • адрес подключения; • SID сервера; • ID сессии; • описание ошибки
Начато построение отчета	280	Запущен процесс формирования отчета. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • тип; • агенты
Ошибка начала построения отчета	281	Во время запущенного процесса формирования отчета произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • тип; • агенты; • описание ошибки
Построение отчета успешно завершено	282	Формирование отчета успешно завершено. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • тип; • агенты
Ошибка построения отчета	283	Во время формирования отчета произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • тип; • агенты; • описание ошибки

Название	ID	Описание
Отмена процесса построения отчета	290	Отмена процесса формирования отчета. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • тип; • агенты
Ошибка отмены процесса построения отчета	291	Во время отмены процесса формирования отчета произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • тип; • агенты; • описание ошибки
Получение расширенной информации об агенте ОУ	300	Запущен процесс получения расширенной информации об агенте оперативного управления. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • имя агента; • ID агента; • тип агента; • класс агента
Ошибка получения расширенной информации об агенте ОУ	301	Во время запущенного процесса получения расширенной информации об агенте оперативного управления произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • имя агента; • ID агента; • тип агента; • класс агента; • описание ошибки
Изменение лицензии	400	Изменение лицензии на использование компонентов системы Secret Net Studio. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • (добавлены| удалены| изменены) лицензии
Ошибка при изменении лицензии	401	Во время изменения лицензии на использование компонентов системы Secret Net Studio произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • (добавлены| удалены| изменены) лицензии; • описание ошибки

Название	ID	Описание
Изменение настроек сервера	500	Изменение настроек сервера безопасности. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • настройка
Ошибка при изменении настроек сервера	501	Во время изменения настроек сервера безопасности произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • SID компьютера; • настройка; • описание ошибки
Изменение групповых политик домена безопасности	502	Изменение групповых политик домена безопасности. В поле "Описание" указываются: • пользователь; • SID пользователя; • имя компьютера; • SID компьютера; • изменены групповые политики для объектов
Ошибка при изменении групповых политик домена безопасности	503	Во время изменения групповых политик домена безопасности произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • имя компьютера; • SID компьютера; • изменены групповые политики для объектов; • описание ошибки
Запрос групповых политик домена безопасности	504	Отправлен запрос групповых политик домена безопасности. В поле "Описание" указываются: • имя компьютера; • SID компьютера; • групповые политики
Ошибка при запросе групповых политик домена безопасности	505	Во время запроса групповых политик домена безопасности произошла ошибка. В поле "Описание" указываются: • имя компьютера; • SID компьютера; • групповые политики; • описание ошибки
Начато уведомление агентов об изменении групповых политик домена безопасности	506	Запущен процесс уведомления агентов об изменении групповых политик домена безопасности. В поле "Описание" указываются: • серверы; • контейнеры AD
Ошибка начала уведомления агентов об изменении групповых политик домена безопасности	507	Во время запущенного процесса уведомления агентов об изменении групповых политик домена безопасности произошла ошибка. В поле "Описание" указываются: • серверы; • контейнеры AD; • описание ошибки

Название	ID	Описание
Уведомление агентов об изменении групповых политик домена безопасности успешно завершено	508	Уведомление агентов об изменении групповых политик домена безопасности успешно завершено. В поле "Описание" указываются: • серверы; • контейнеры AD
Ошибка уведомления агентов об изменении групповых политик домена безопасности	509	Во время уведомления агентов об изменении групповых политик домена безопасности произошла ошибка. В поле "Описание" указываются: • серверы; • контейнеры AD; • описание ошибки
Уведомление об изменении настроек родительского сервера	510	Уведомление об изменении настроек родительского сервера безопасности. В поле "Описание" указываются: • SID сервера; • настройка
Ошибка уведомления об изменении настроек родительского сервера	511	Во время уведомления об изменении настроек родительского сервера безопасности произошла ошибка. В поле "Описание" указываются: • SID сервера; • настройка; • описание ошибки
Изменение задания оперативного управления	512	Изменение задания оперативного управления. В поле "Описание" указываются: • пользователь; • SID пользователя; • действие; • ID задания; • категория; • номер; • команда; • версия ПО; • количество компьютеров
Ошибка изменения задания оперативного управления	513	Во время изменения задания оперативного управления произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • действие; • ID задания; • категория; • номер; • команда; • версия ПО; • количество компьютеров; • описание ошибки
Изменение в репозитории	514	Изменение в репозитории. В поле "Описание" указываются: • пользователь; • SID пользователя; • действие; • версия ПО; • категория ПО

Название	ID	Описание
Ошибка работы с репозиторием	515	Во время работы с репозиторием произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • действие; • версия ПО; • категория ПО; • описание ошибки
Изменение в конфигурации межсетевого экрана	516	Изменение в конфигурации межсетевого экрана. Пользователь указан в поле "Описание"
Ошибка работы с конфигурацией межсетевого экрана	517	Во время работы с конфигурацией межсетевого экрана произошла ошибка. В поле "Описание" указываются: • пользователь; • описание ошибки
Начато развертывание ПО	518	Запущен процесс установки программного обеспечения на рабочую станцию. В поле "Описание" указываются: • имя компьютера; • SID компьютера; • версия ПО; • ID задания
Завершено развертывание ПО	519	Процесс установки программного обеспечения на рабочую станцию успешно завершен. В поле "Описание" указываются: • имя компьютера; • SID компьютера; • версия ПО; • ID задания
Ошибка развертывания ПО	520	Во время установки программного обеспечения на рабочую станцию произошла ошибка. В поле "Описание" указываются: • имя компьютера; • SID компьютера; • версия ПО; • ID задания; • описание ошибки
Начато удаление ПО	525	Запущен процесс удаления программного обеспечения на рабочей станции. В поле "Описание" указываются: • имя компьютера; • SID компьютера; • версия ПО; • ID задания
Завершено удаление ПО	526	Процесс удаления программного обеспечения на рабочей станции успешно завершен. В поле "Описание" указываются: • имя компьютера; • SID компьютера; • версия ПО; • ID задания
Команда управления JaCarta	527	Запущен процесс выполнения команды управления JaCarta
Ошибка команды управления JaCarta	528	Во время запущенного процесса выполнения команды управления JaCarta произошла ошибка. Описание ошибки указано в поле "Описание"

Название	ID	Описание
После репликации обнаружено новое повреждение конфигурации	600	После копирования данных обнаружено новое повреждение конфигурации. В поле "Описание" указываются: • потерянные агенты; • агенты-дубликаты; • потерянные серверы; • серверы-дубликаты
Повреждение конфигурации не обнаружено после репликации	601	Повреждение конфигурации не обнаружено после копирования данных. В поле "Описание" указываются: • потерянные агенты; • агенты-дубликаты; • потерянные серверы; • серверы-дубликаты
Команда удаления поврежденной записи из LDS	602	Команда удаления поврежденной записи из LDS. Удаленные объекты LDS указаны в поле "Описание"
Репликация конфигурации ОУ	603	Копирование конфигурации оперативного управления. В поле "Описание" указываются: • компьютер; • SID компьютера; • список идентификаторов измененных объектов управления: агентов и серверов
Ошибка репликации конфигурации ОУ	604	Во время копирования конфигурации оперативного управления произошла ошибка. В поле "Описание" указываются: • компьютер; • SID компьютера; • список идентификаторов измененных объектов управления: агентов и серверов; • описание ошибки
Утверждение паспорта ПО	605	Утверждение паспорта программного обеспечения рабочей станции. В поле "Описание" указываются: • пользователь; • SID пользователя; • объект(ы)
Ошибка утверждения паспорта ПО	606	Во время утверждения паспорта программного обеспечения рабочей станции произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • объект(ы); • описание ошибки
Удаление паспорта ПО	607	Удаление паспорта программного обеспечения рабочей станции. В поле "Описание" указываются: • пользователь; • SID пользователя; • объект(ы)
Ошибка удаления паспорта ПО	608	Во время удаления паспорта программного обеспечения рабочей станции произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • объект(ы); • описание ошибки

Название	ID	Описание
Загрузка проекта паспорта ПО из файла	609	Загрузка проекта паспорта программного обеспечения рабочей станции из файла. В поле "Описание" указываются: • пользователь; • SID пользователя; • объект(ы)
Ошибка загрузки проекта паспорта ПО	610	Во время загрузки проекта паспорта программного обеспечения рабочей станции произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • объект(ы); • описание ошибки
Синхронизация паспортов ПО	611	Синхронизация паспортов программного обеспечения рабочей станции. В поле "Описание" указываются: • пользователь; • SID пользователя
Ошибка синхронизации паспортов ПО	612	Во время синхронизации паспортов программного обеспечения рабочей станции произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • описание ошибки
Запуск сбора данных СПС	613	Запущен процесс сбора данных о состоянии программной среды рабочей станции. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер(ы)
Сбор данных СПС завершен	614	Сбор данных о состоянии программной среды рабочей станции завершен. В поле "Описание" указываются: • пользователь; • SID пользователя; • объект(ы)
Ошибка в процессе сбора данных СПС	615	Во время процесса сбора данных о состоянии программной среды рабочей станции произошла ошибка. В поле "Описание" указываются: • пользователь; • SID пользователя; • компьютер; • описание ошибки
Ошибка в процессе чтения данных из БД	616	Во время процесса чтения данных из базы данных сервера безопасности произошла ошибка. Описание ошибки указано в поле "Описание"
Ошибка в процессе чтения конфигурации из хранилища	617	Во время процесса чтения конфигурации из хранилища произошла ошибка
Создание подписанного контейнера для исходящего шлюза	618	Получение файла шлюза. В поле "Описание" указываются: • пользователь; • SID пользователя; • идентификатор шлюза; • имя шлюза

Название	ID	Описание
Ошибка создания подписанного контейнера для исходящего шлюза	619	Произошла ошибка во время получения файла шлюза. В поле "Описание" указываются: • пользователь; • SID пользователя; • идентификатор шлюза; • имя шлюза; • описание ошибки
Создание в конфигурации входящего шлюза	620	Запущена процедура создания входящего шлюза в конфигурации. В поле "Описание" указываются: • пользователь; • SID пользователя; • идентификатор шлюза; • имя шлюза; • имя сервера за шлюзом; • полная синхронизация; • частичная синхронизация
Ошибка создания в конфигурации входящего шлюза	621	Произошла ошибка при создании входящего шлюза в конфигурации. В поле "Описание" указываются: • пользователь; • SID пользователя; • идентификатор шлюза; • имя шлюза; • имя сервера за шлюзом; • полная синхронизация; • частичная синхронизация; • описание ошибки
Обновление свойств шлюза	622	Редактирование информации шлюза. В поле "Описание" указываются: • пользователь; • SID пользователя; • идентификатор шлюза; • имя шлюза; • полная синхронизация; • частичная синхронизация
Ошибка обновления свойств шлюза	623	Произошла ошибка при редактировании информации шлюза. В поле "Описание" указываются: • пользователь; • SID пользователя; • идентификатор шлюза; • имя шлюза; • полная синхронизация; • частичная синхронизация; • описание ошибки
Удаление шлюза из конфигурации	624	Запущена процедура удаления шлюза из конфигурации. В поле "Описание" указываются: • пользователь; • SID пользователя; • идентификатор шлюза; • имя шлюза
Ошибка удаления шлюза из конфигурации	625	Произошла ошибка при удалении шлюза из конфигурации. В поле "Описание" указываются: • пользователь; • SID пользователя; • идентификатор шлюза; • имя шлюза; • описание ошибки

Название	ID	Описание
Принудительная синхронизация шлюза	626	Запущена процедура принудительной синхронизации шлюза. В поле "Описание" указываются: • пользователь; • SID пользователя; • идентификатор шлюза; • имя шлюза; • полная синхронизация; • частичная синхронизация
Ошибка принудительной синхронизации шлюза	627	Произошла ошибка при принудительной синхронизации шлюза. В поле "Описание" указываются: • пользователь; • SID пользователя; • идентификатор шлюза; • имя шлюза; • полная синхронизация; • частичная синхронизация; • описание ошибки
Запрос ключей восстановления	628	Запущена процедура запроса ключей восстановления В поле "Описание" указываются: • пользователь; • SID пользователя; • привязка; • подчинение; • подсистема;
Ошибка запроса ключей восстановления	629	Произошла ошибка при запросе ключей восстановления В поле "Описание" указываются: • пользователь; • SID пользователя; • привязка; • подчинение; • подсистема; • описание ошибки
Добавление нового криптографического ключа	630	Запущена процедура добавления нового криптографического ключа В поле "Описание" указываются: • пользователь; • SID пользователя; • новый ключ; • комментарий; • архивные ключи
Ошибка добавления нового криптографического ключа домена	631	Произошла ошибка при добавлении нового криптографического ключа В поле "Описание" указываются: • пользователь; • SID пользователя; • ключ; • описание ошибки
Обновление криптографического ключа домена	632	Запущена процедура обновления криптографического ключа домена В поле "Описание" указываются: • пользователь; • SID пользователя; • старый комментарий; • новый комментарий
Ошибка обновления криптографического ключа домена	633	Произошла ошибка при обновлении криптографического ключа домена В поле "Описание" указываются: • пользователь; • SID пользователя; • ключ; • описание ошибки

Название	ID	Описание
Удаление криптографического ключа домена	634	Запущена процедура удаления криптографического ключа домена В поле "Описание" указываются: • пользователь; • SID пользователя; • удалённый ключ; • комментарий удалённого ключа; • активный ключ; • комментарий активного ключа; • архивные ключи
Ошибка удаления криптографического ключа домена	635	Произошла ошибка при удалении криптографического ключа домена В поле "Описание" указываются: • пользователь; • SID пользователя; • ключ; • описание ошибки
Обновление ключа восстановления	636	Запущена процедура обновления ключа восстановления В поле "Описание" указываются: • пользователь; • SID пользователя; • ключ; • подсистема; • устаревший комментарий; • новый комментарий
Ошибка обновления ключа восстановления	637	Произошла ошибка при обновлении ключа восстановления В поле "Описание" указываются: • пользователь; • SID пользователя; • ключ; • описание ошибки
Удаление ключа восстановления	638	Запущена процедура удаления ключа восстановления В поле "Описание" указываются: • удалённый ключ; • подсистема; • привязка; • Идентификатор связанного объекта; • Имя связанного объекта; • комментарий удалённого ключа
Ошибка удаления ключа восстановления	639	Произошла ошибка при удалении ключа восстановления В поле "Описание" указываются: • пользователь; • SID пользователя; • ключ; • описание ошибки
Обнаружение криптографического ключа домена при обновлении конфигурации	640	При обновлении конфигурации обнаружен криптографический ключ домена В поле "Описание" указываются: • активный ключ; • комментарий активного ключа; • архивные ключи
Исчезновение криптографического ключа домена при обновлении конфигурации	641	При обновлении конфигурации исчез криптографический ключ домена В поле "Описание" указываются: • удалённый ключ; • комментарий удалённого ключа; • активный ключ; • комментарий активного ключа; • архивные ключи

Название	ID	Описание
Деактивация лицензий	642	Отправлен запрос на деактивацию лицензий В поле "Описание" указываются: • пользователь; • SID пользователя; • идентификаторы лицензий; • идентификаторы активаций
Ошибка деактивации лицензий	643	Произошла ошибка при деактивации лицензий В поле "Описание" указываются: • пользователь; • SID пользователя; • идентификаторы лицензий; • описание ошибки
Обнаружение изменения чёрного списка лицензий после репликации	644	После репликации было обнаружено изменение чёрного списка В поле "Описание" указываются: • количество лицензий в списке; • скомпрометированные серверы

Документация

1. Средство защиты информации Secret Net Studio – C. Руководство администратора. Установка, управление, мониторинг и аудит	RU.88338853.501400.002 91 1
2. Средство защиты информации Secret Net Studio – C. Руководство администратора. Настройка и эксплуатация	RU.88338853.501400.002 91 2
3. Средство защиты информации Secret Net Studio – C. Руководство пользователя	RU.88338853.501400.002 92